Performance Counters and Alerts

System Counters

Cisco HAProxy

The HAProxy object offers proxy capabilities for HTTP-based applications. This object frontend all the incoming web traffic into Unified Communication Manager and IM and Presence Service.

HAProxy handles all the HTTP/HTTPS requests and provides improved Tomcat stability through offloading of crypto functionality.

The following table contains information about the HAProxy counters.

Table 1: Cisco HAProxy

Counters	Counter Description
TotalDeniedRequests	The total number of denied requests since the process started.
TotalDeniedResponse	The total number of denied responses since the process started.
Econ	The total number of failed connections to the server since the process st
TimeInQueue	The average time measured in milliseconds spent by the requests in the counter measure is averaged upto the last 1024 requests on the backend

Counters	Counter Description
TotalRequestAndResponseTime	The total time spent for processing the agent requests and response time. It the request time, no. of connections in the queue, their response, and the total time. This counter measure is averaged upto the last 1024 requests on the b server.

Cisco Tomcat Connector

The Tomcat Hypertext Transport Protocol (HTTP) and HTTP Secure (HTTPS) Connector object provides information about Tomcat connectors.

A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when application web pages are accessed. The Secure Socket Layer (SSL) status of web application URLs provides the basis for the instance name for each Tomcat HTTP Connector. For example, `https://<IP Address>:8443` for SSL or `http://<IP Address>:8080` for non-SSL.

The following table contains information about the Tomcat HTTP connector counters.

Table 2: Cisco Tomcat Connector

Counters	Counter Description
Errors	The total number of HTTP errors (for example, `401 Unauthorized`) that the encountered.
MBytesReceived	The amount of data that the connector received.
MBytesSent	The amount of data that the connector sent.
Requests	The total number of request that the connector handled.
ThreadsTotal	The current total number of request processing threads, including available threads, for the connector.
ThreadsMax	The maximum number of request processing threads for the connector. Each incoming request on a web application window requires a thread for th of that request. If more simultaneous requests are received than the currently request processing threads can handle, additional threads are created up to the maximum shown in this counter. If still more simultaneous requests are rece accumulate within the server socket that the connector created, up to an int specified maximum number. Any further simultaneous requests receive co refused messages until resources are available to process them.
ThreadsBusy	This counter represents the current number of busy/in-use request processi for the connector.

Cisco Tomcat JVM

The Cisco Tomcat Java Virtual Machine (JVM) object provides information about the pool of common resource memory used by web applications such as Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and Cisco Unity Connection Administration. The dynamic memory block stores all objects that Tomcat and its web applications create.

The following table contains information about the Tomcat JVM counters.

Table 3: Tomcat JVM

Counters	Counter Description
KBytesMemoryFree	The amount of free dynamic memory block (heap memory) in the Tomca Machine. When the amount of free dynamic memory is low, more memory is aut allocated, and total memory size (represented by the KbytesMemoryTo increases but only up to the maximum (represented by the KbytesMemory You can determine the amount of memory in use by subtracting KBytes from KbytesMemoryTotal.
KBytesMemoryMax	The amount of free dynamic memory block (heap memory) in the Tomca Machine.
KBytesMemoryTotal	The current total dynamic memory block size, including free and in-use Tomcat Java Virtual Machine.

Cisco Tomcat Web Application

The Cisco Tomcat Web Application object provides information about how to run web applications.

The URLs for the web application provide the basis for the instance name for each Tomcat Web Application, as explained in the following examples:

- Cisco Unified Communications Manager Administration (`https://<IP Address>:8443/ccmadmin`) is identified by `ccmadmin`.
- Cisco Unified Serviceability (`https://<IP Address>:8443/ccmservice`) is identified by `ccmservice`.
- Cisco Unified Communications Manager User Options (`https://<IP Address>:8443/ccmuser`) is identified by `ccmuser`.
- Cisco Unity Connection Administration (`https://<IP Address>:8443/cuadmin`) is identified by `cuadmin`.
- URLs that do not have an extension, such as `https://<IP Address>:8443` or `http://<IP Address>:8080`), are identified by _root.

The following table contains information on the Tomcat Web Application counters.

Table 4: Tomcat Web Application

Counters	Counter Description
Errors	The total number of HTTP errors (for example, 401 Unauthorized) that a U Communications Manager-related or Cisco Unity Connection-related web a encounters.
Requests	The total number of requests that the web application handles. Each time th application is accessed, its Requests counter increments accordingly.
SessionsActive	The number of active or in use sessions in the web application.

Cisco UDS Tomcat Connector

The UDS Tomcat Hypertext Transport Protocol (HTTP) and HTTP Secure (HTTPS) Connector object provides information about Tomcat connectors.

A UDS Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when application web pages are accessed. The Secure Socket Layer (SSL) status of web application URLs provides the basis for the instance name for each UDS Tomcat HTTP Connector. For example, `https://<IP Address>:8443` for SSL or `http://<IP Address>:8080` for non-SSL.

The following table contains information about the UDS Tomcat HTTP connector counters.

Table 5: Cisco UDS Tomcat Connector

Counters	Counter Description
Errors	The total number of HTTP errors (for example, `401 Unauthorized`) that the encountered.
MBytesReceived	The amount of data that the connector received.
MBytesSent	The amount of data that the connector sent.
Requests	The total number of request that the connector handled.
ThreadsBusy	This counter represents the current number of busy/in-use request processi for the connector.
ThreadsTotal	The current total number of request processing threads, including available threads, for the connector.

Counters	Counter Description
ThreadsMax	The maximum number of request processing threads for the connector. Each incoming request on a web application window requires a thread fo of that request. If more simultaneous requests are received than the curre request processing threads can handle, additional threads are created up to t maximum shown in this counter. If still more simultaneous requests are accumulate within the server socket that the connector created, up to an specified maximum number. Any further simultaneous requests receive refused messages until resources are available to process them.

Cisco UDS Tomcat JVM

The Cisco UDS Tomcat Java Virtual Machine (JVM) object provides information about the UDS Tomcat JVM, which represents, among common things, a pool of common resource memory used by Cisco Unified Communications Manager-related web applications such as UDS, tomcatstats, and more.

The following table contains information about the UDS Tomcat JVM counters.

Table 6: Cisco UDS Tomcat JVM

Counters	Counter Description
KBytesMemoryFree	The amount of free dynamic memory block (heap memory) in the UDS Virtual Machine. When the amount of free dynamic memory is low, more memory is aut allocated, and total memory size (represented by the KbytesMemoryTo increases but only up to the maximum (represented by the KbytesMemory You can determine the amount of memory in use by subtracting KBytes from KbytesMemoryTotal.
KBytesMemoryMax	The amount of free dynamic memory block (heap memory) in the UDS Virtual Machine.
KBytesMemoryTotal	The current total dynamic memory block size, including free and in-use UDS Tomcat Java Virtual Machine.

Cisco UDS Tomcat Web Application

The Cisco UDS Tomcat Web Application object provides information about how to run Unified Communications Manager web applications.

The URLs for the web application provide the basis for the instance name for each Tomcat Web Application, as explained in the following examples:

- Cisco Unified Communications Manager Administration (`https://<IP Address>:8443/ccmadmin`) is identified by `ccmadmin`.
- Cisco Unified Serviceability (`https://<IP Address>:8443/ccmservice`) is identified by `ccmservice`.

- Cisco Unified Communications Manager User Options (`https://<IP Address>:8443/ccmuser`) is identified by `ccmuser`.
- Cisco Unity Connection Administration (`https://<IP Address>:8443/cuadmin`) is identified by `cuadmin`.
- URLs that do not have an extension, such as `https://<IP Address>:8443` or `http://<IP Address>:8080`), are identified by _root.

The following table contains information on the UDS Tomcat Web Application counters.

Table 7: Cisco UDS Tomcat Web Application

Counters	Counter Description
Errors	The total number of HTTP errors (for example, 401 Unauthorized) that a U Communications Manager-related or Cisco Unity Connection-related web a encounters.
Requests	The total number of requests that the web application handles. Each time th application is accessed, its Requests counter increments accordingly.
SessionsActive	The number of active or in use sessions in the web application.

Database Change Notification Client

The Database Change Notification Client object provides information about change notification clients. The following table contains information about the Database Change Notification Client counters.

Table 8: Database Change Notification Client

Counters	Counter Descriptions
MessagesProcessed	The number of database change notifications that have been processed. Thi refreshes every 15 seconds.
MessagesProcessing	The number of change notification messages that are currently being proces waiting to be processed in the change notification queue for this client. Thi refreshes every 15 seconds.
QueueHeadPointer	The head pointer to the change notification queue. The head pointer acts as th point in the change notification queue. To determine the number of notificat queue, subtract the head pointer value from the tail pointer value. By defau counter refreshes every 15 seconds.
QueueMax	The largest number of change notification messages that will be processed client. This counter remains cumulative since the last restart of the Cisco D Layer Monitor service.
QueueTailPointer	The tail pointer to the change notification queue. The tail pointer represents t point in the change notification queue. To determine the number of notificat queue, subtract the head pointer value from the tail pointer value. By defau counter refreshes every 15 seconds

Counters	Counter Descriptions
TablesSubscribed	The number of tables in which this client has subscribed.

Database Change Notification Server

The Database Change Notification Server object provides information about different change-notification-related statistics. The following table contains information about the Database Change Notification Server counters.

Table 9: Database Change Notification Server

Counter	Counter Descriptions
Clients	The number of change notification clients (services and servlets) that ha for change notification.
CNProcessed	The total number of change notification messages processed by the serve
Queue Delay	The number of seconds that the change notification process has messag but is not processing them. This condition is true if: • either Change Notification Requests Queued in Database (QueuedR and Change Notification Requests Queued in Memory (QueuedRequestsInMemory) are non-zero, or • the Latest Change Notification Messages Processed count is not ch This condition is checked every 15 seconds.
QueuedRequestsInDB	The number of change notification records that are in the DBCNQueue Change Notification Queue) table through direct TCP/IP connection (n shared memory). This counter refreshes every 15 seconds.
QueuedRequestsInMemory	The number of change notification requests that are queued in shared m

Database Change Notification Subscription

The Database Change Notification Subscription object displays the names of tables where the client receives Change Notifications.

The SubscribedTable object displays the table with the service or servlet that receives change notifications. Because the counter does not increment, this display occurs for informational purposes only.

Database Local DSN

The Database Local Data Source Name (DSN) object and LocalDSN counter provide the DSN information for the local machine. The following table contains information on the Database local DSN.

Table 10: Database Local Data Source Name

Counters	Counter Descriptions
CcmDbSpace_Used	The amount of Ccm DbSpace that is consumed
CcmtempDbSpace_Used	The amount of Ccmtemp DbSpace that is consumed.
CNDbSpace_Used	The percentage of CN DbSpace that is consumed.
LocalDSN	The DSN that is being referenced from the local machine.
SharedMemory_Free	The total shared memory that is free.
SharedMemory_Used	The total shared memory that is used.
RootDbSpace_Used	The amount of RootDbSpace that is consumed.

DB User Host Information Counters

The DB User Host Information object provides information about DB User Host.

The DB:User:Host Instance object displays the number of connections that are present for each instance of DB:User:Host.

Enterprise Replication DBSpace Monitors

The enterprise replication DBSpace monitors object displays the usage of various ER DbSpaces. The following table contains information about the enterprise replication DB monitors.

Table 11: Enterprise Replication DBSpace Monitors

Counters	Counter Descriptions
ERDbSpace_Used	The amount of enterprise replication DbSpace that was consumed.
ERSBDbSpace_Used	The amount of ERDbSpace that was consumed.

Enterprise Replication Perfmon Counters

The Enterprise Replication Perfmon Counter object provides information about the various replication counters.

The ServerName:ReplicationQueueDepth counter displays the server name followed by the replication queue depth.

IP

The IP object provides information on the IPv4-related statistics on your system. The following table contains information about the IP counters.

Note These counters are also part of the IP6 object, which supports Unified Communications Manager and provides information about the IPv6-related statistics on your system.

Table 12: IP Counters

Counters	Counter Descriptions
Frag Creates	The number of IP datagrams fragments that are generated at this entity.
Frag Fails	The number of IP datagrams that are discarded at this entity because th cannot be fragmented, such as datagrams where the Do not Fragment fl
Frag OKs	The number of IP datagrams that are successfully fragmented at this en
In Delivers	The number of input datagrams that are delivered to IP user protocols. includes Internet Control Message Protocol (ICMP).
In Discards	The number of input IP datagrams where no issues are encountered, bu discarded. One possible reason is a lack of buffer space. This counter do any datagrams that are discarded while awaiting reassembly.
In HdrErrors	The number of input datagrams that are discarded with header errors. T includes bad checksums, version number mismatch, other format errors exceeded, and other errors that are discovered in processing their IP opt
In Receives	The number of input datagrams that are received from all network inter counter includes datagrams that were received with errors
In UnknownProtos	The number of locally addressed datagrams that are received successfully because of an unknown or unsupported protocol.
InOut Requests	The number of incoming IP datagrams that are received and the numbe IP datagrams that are sent.
Out Discards	The number of output IP datagrams that are not transmitted and are disc possible reason is a lack of buffer space.
Out Requests	This counter represents the total number of IP datagrams that local IP u (including ICMP) supply to IP in requests transmission. This counter do any datagrams that were counted in ForwDatagrams.
Reasm Fails	The number of IP reassembly failures that the IP reassembly algorithm including time outs and errors. This counter does not represent the discarded IP fragments because som such as the algorithm in RFC 815, can lose track of the number of fragn these algorithms combine fragments as they are received.
Reasm OKs	The number of IP datagrams that are successfully reassembled.

Counters	Counter Descriptions
Reasm Reqds	The number of IP fragments that are received that require reassembly at thi

Memory

The memory object provides information about the usage of physical memory and swap memory on the server. The following table contains information about memory counters.

Table 13: Memory

Counters	Counter Descriptions
% Mem Used	Displays the system physical memory utilization as a percentage. The valu counter is calculated as follows: `Total KBytes - Free KBytes - Buffers KBytes - Cached + Shared KBytes) / Total KBytes` This value also corresponds to the Used KBytes/Total KBytes
% Page Usage	The percentage of active pages.
% VM Used	Displays the system virtual memory utilization as a percentage. The value counter is calculated as follows: `Total KBytes - Free KBytes - Buffers KBytes - Cached + Shared KBytes + Used Swap KBytes) / (Total KBytes Swap KBytes)` This value also corresponds to Used VM KBytes/Total VM KBytes.
Buffers KBytes	The capacity of buffers in your system in kilobytes.
Cached KBytes	The amount of cached memory in kilobytes.
Free KBytes	The total amount of memory that is available in your system in kilobytes.
Free Swap KBytes	The amount of free swap space that is available in your system in kilobytes
HighFree	The amount of free memory in the high region. The Linux kernel splits the virtual memory address space into memory regi high memory is memory above a certain physical address, and its amount d the total memory and the type of kernel on the system. For the Unified Communications Manager system with 4 GB memory, the hig is roughly in the address of 896M to 4096M.

Counters	Counter Descriptions
HighTotal	The total amount of memory in the high region. The Linux kernel splits the virtual memory address space into memory high memory is memory above a certain physical address, and its amou the total memory and the type of kernel on the system. For the Unified Communications Manager system with 4 GB memory, the is roughly in the address of 896M to 4096M.
Page Faults Per Sec	The number of page faults (both major and minor) that the system mak (post 2.5 kernels only). This reading does not necessarily represent a co faults that generate input and output (I/O) because some page faults can without I/O.
Low Total	The total low (non-paged) memory for kernel.
Low Free	The total free low (non-paged) memory for kernel.
Page Major Faults Per Sec	The number of major faults that the system makes per second that requi page from the disk (post 2.5 kernels only).
Pages	The number of pages that the system pages in from the disk, plus the nu that the system pages out to the disk.
Pages Input	The number of pages that the system pages in from the disk.
Pages Input Per Sec	The total number of kilobytes that the system pages in from the disk pe
Pages Output	The number of pages that the system pages out to the disk.
Pages Output Per Sec	The total number of kilobytes that the system pages out to the disk per s
Shared KBytes	The amount of shared memory in your system in kilobytes.
SlabCache	The memory used by created slabcaches by various kernel components, macroscopic counter representing the sum of all the individual entries i slabinfo.
SwapCached	The amount of Swap used as cache memory. Memory that once was sw swapped back in, but is still in the swapfile.
Total KBytes	The total amount of memory in your system in kilobytes.
Total Swap KBytes	The total amount of swap space in your system in kilobytes.
Total VM KBytes	The total amount of system physical and memory and swap space (Tota Total Swap Kbytes) that is in use in your system in kilobytes.

Counters	Counter Descriptions
Used KBytes	The amount of in-use physical memory. The value of the Used KBytes cou calculated as follows: `Total KBytes - Free KBytes - Buffers KBytes - Cached + Shared KBytes.` The Used KBytes value differs from the Linux term that displays in the top command output. The Used value that displays in the top or free command equals the difference in Total KBytes - Free KBytes and also includes the s Buffers KBytes and Cached KBytes.
Used Swap KBytes	This counter represents the amount of swap space that is in use on your sys kilobytes.
Used VM KBytes	This counter represents the system physical memory and the amount of swa that is in use on your system in kilobytes. The value is calculated as follow `Total KBytes - Free KBytes - Buffers KBytes - Cached + Shared KBytes + Used Swap KBytes` This value corresponds to Used Mem KBytes + Used Swap KBytes.

Network Interface

The network interface object provides information about the network interfaces on the system. The following table contains information about network interface counters.

Table 14: Network Interface

Counters	Counter Descriptions
Rx Bytes	The number of bytes, including framing characters that are received on this
Rx Dropped	The number of inbound packets that are chosen to be discarded even though have been detected. This action prevents the packet from being delivered to higher-layer protocol. Discarding packets also frees up buffer space.
Rx Errors	The number of inbound packets (packet-oriented interfaces) and the number o transmission units (character-oriented or fixed-length interfaces) that conta that prevented them from being delivered to a higher-layer protocol.
Rx Multicast	The number of multicast packets that are received on this interface.
Rx Packets	The number of packets that this sublayer delivered to a higher sublayer. Thi does not include the packets that are addressed to a multicast or broadcast a this sublayer.
Total Bytes	The total number of received (Rx) bytes and transmitted (Tx) bytes.
Total Packets	The total number of Rx packets and Tx packets.

Counters	Counter Descriptions
Tx Bytes	The total number of octets, including framing characters, that are transm the interface.
Tx Dropped	The number of outbound packets that are chosen to be discarded even tho are detected. This action prevents the packet from being delivered to a l protocol. Discarding a packet also frees up buffer space.
Tx Errors	The number of outbound packets (packet-oriented interfaces) and the nu outbound transmission units (character-oriented or fixed-length interfac transmitted because of errors.
Tx Packets	The total number of packets that the higher-level protocols requested for including those that are discarded or not sent. This situation doesn't incl that are addressed to a multicast or broadcast address at this sublayer.
Tx QueueLen	The length of the output packet queue (in packets).

Number of Replicates Created and State of Replication

The Number of Replicates Created and State of Replication object provides real-time replication information for the system. The following table contains information about replication counters.

Table 15: Number of Replicates Created and State of Replication

Counters	Counter Descriptions
Number of Replicates Created	The number of replicates that are created by Informix for the DB tables displays information during Replication Setup.
Replicate_State	The state of replication. The following list provides possible values: **0** Initializing. The counter equals 0 when the server is not defined or w is defined but realizes the template has not completed. **1** Replication setup script fired from this node. Cisco recommends tha **dbreplication status** on the CLI to determine the location and caus **2** Good Replication. **3** Bad Replication. A counter value of 3 indicates replication in the c It does not mean that replication failed on a particular server in the recommends that you run **utils dbreplication status** on the CLI the location and cause of the failure. **4** Replication setup did not succeed.

Partition

The partition object provides information about the file system and its usage in the system. The following table contains information about partition counters. These counters are also available for the spare partition, if present.

Table 16: Partition

Counters	Counter Descriptions
% CPU Time	The percentage of CPU time that is dedicated to handling IO requests that w to the disk.
% Used	The percentage of disk space that is in use on this file system.
% Wait in Read	Not Used. The Await Read Time counter replaces this counter. This counte longer valid with the counter value -1.
% Wait in Write	Not Used. The Await Write Time counter replaces this counter. This counte longer valid with the counter value -1.
Await Read Time	The average time measured in milliseconds for read requests that are issue device to be served.
Await Time	The average time measured in milliseconds for input and output (I/O) reque issued to the device to be served. This reading includes the time spent by th in queue and the time spent servicing them.
Await Write Time	The average time measured in milliseconds for write requests that are issue device to be served.
Queue Length	The average queue length for the requests that are issued to the disk.
Read Bytes Per Sec	The amount of data in bytes per second that is read from the disk.
Total Mbytes	The amount of total disk space in megabytes that is on this file system.
Used Mbytes	The amount of disk space in megabytes that is in use on this file system.
Write Bytes Per Sec	The amount of data that is written to the disk in bytes per second.

Process

The process object provides information about the processes that are running on the system. The following table contains information about process counters.

Table 17: Process

Counters	Counter Descriptions
% CPU Time	This counter, which is expressed as a percentage of total central processing u time, represents the tasks share of the elapsed CPU time since the last upda

Counters	Counter Descriptions
% MemoryUsage	This counter represents the percentage of physical memory that a task i using.
Data Stack Size	This counter represents the stack size for task memory status.
Nice	This counter represents the nice value of the task. • A negative nice value indicates that the process has a higher priori • A positive nice value indicates that the process has a lower priority **Note** If the nice value equals zero, do not adjust the priority whe determining the dispatchability of a task.
Page Fault Count	This counter represents the number of major page faults that a task enc requires the data to be loaded into memory.
PID	This counter displays the task-unique process ID. The ID periodically v value never equals zero.
Process Status	This counter displays the process status: **0** Running **1** Sleeping **2** Uninterruptible disk sleep **3** Zombie **4** Stopped **5** Paging **6** Unknown
Shared Memory Size	This counter displays the amount of shared memory in kilobytes (KB) t using. Other processes could potentially share the same memory.
STime	This counter displays the system time (STime), measured in jiffies, that has scheduled in kernel mode. A jiffy corresponds to a unit of CPU tim as a base of measurement. One second comprises 100 jiffies.

Counters	Counter Descriptions
Thread Count	This counter displays the number of threads that are currently grouped with negative value (-1) indicates that this counter is currently not available. Thi happens when thread statistics (which include all performance counters in t object as well as the Thread Count counter in the Process object) are turned o the system total processes and threads exceed the default threshold value.
Total CPU Time Used	This counter displays the total CPU time in jiffies that the task used in user kernel mode since the task started.
UTime	This counter displays the time, measured in jiffies, that a task has schedule mode.
VmData	This counter displays the virtual memory usage of the heap for the task in K
VmRSS	This counter displays the virtual memory (Vm) resident set size (RSS) that is in physical memory in KB. This reading includes the code, data, and stack.
VmSize	This counter displays the total virtual memory usage for a task in KB. This includes all code, data, shared libraries, and pages that have been swapped Virtual Image = swapped size + resident size
Wchan	This counter displays the channel (system call) in which the process is wait

Processor

The processor object provides information about different processor time usage in percentages. The following table contains information about processor counters.

Table 18: Processor

Counters	Counter Descriptions
% CPU Time	This counter displays the processors share of the elapsed central processing u time, excluding idle time, since the last update. This share is expressed as a p of total CPU time.
Idle Percentage	This counter displays the percentage of time that the processor is in the idle does not have an outstanding disk input and output (I/O) request.
IOwait Percentage	This counter represents the percentage of time that the processor is in the id while the system had an outstanding disk I/O request.
Irq Percentage	This counter represents the percentage of time that the processor spends exe interrupt request that is assigned to devices, including the time that the proces sending a signal to the computer.
Nice Percentage	This counter displays the percentage of time that the processor spends execu user level with nice priority.

Counters	Counter Descriptions
Softirq Percentage	This counter represents the percentage of time that the processor spends soft IRQ and deferring task switching to get better CPU performance.
System Percentage	This counter displays the percentage of time that the processor is execut at the system (kernel) level.
User Percentage	This counter displays the percentage of time that the processor is execu processes at the user (application) level.

System

The System object provides information about file descriptors on your system.

The following table contains information about system counters.

Table 19: System

Counters	Counter Descriptions
Allocated FDs	The number of allocated file descriptors.
Being Used FDs	The number of file descriptors that are currently in use in the system.
Freed FDs	The number of allocated file descriptors on the system that are freed.
IOPerSecond	The number of input and output (I/O) operations on all disk partitions p this server. If you experience a system performance issue, use the infor counter to measure the impact of the aggregate I/O operations on this se
IOReadReqMergedPerSecond	The number of read requests merged per second that are queued to all d server.
IOWriteReqMergedPerSecond	The number of write requests merged per second that are queued to all d server.
IOReadReqPerSecond	The number of read requests per second that are issued to all devices or
IOWriteReqPerSecond	The number of write requests per second that are issued to all devices o
IOSectorsReadPerSecond	The number of sectors read per second from all devices on this server.
IOSectorsWrittenPerSecond	The number of sectors written per second to all devices on this server.
IOKBytesReadPerSecond	The number of KBytes read per second from all devices on this server.
IOKBytesWrittenPerSecond	The number of KBytes written per second to all devices on this server.
IOSectorsReqSizeAvg	The average size in sectors of the requests that are issued to all devices
IOReqQueueSizeAvg	The average queue length of the requests that are issued to all devices o

Counters	Counter Descriptions
IOAwait	The average time in milliseconds for I/O requests that are issued to all devi served. This reading includes the time spent by the requests in queue and th spent servicing the requests.
IOServiceTime	The average service time in milliseconds for I/O requests that are issued to a on this server.
IOCpuUtil	The percentage of CPU time during which I/O requests are issued to the de (bandwidth utilization for the device) on this server.
Max FDs	The maximum number of file descriptors that are allowed on the system.
Total CPU Time	The total time in jiffies that the system has been up and running.
Total Processes	The number of processes on the system.
Total Threads	The number of threads on the system.

TCP

The TCP object provides information on the TCP statistics on your system.

The following table contains information about the TCP counters.

Table 20: TCP

Counters	Counter Description
Active Opens	This counter displays the number of times that the TCP connections make a transition to the SYN-SENT state from the CLOSED state.
Attempt Fails	This counter displays the number of times that the TCP connections make a transition to the CLOSED state from either the SYN-RCVD state or the SY state. The counter also displays the number of times TCP connections mak transition to the LISTEN state from the SYS-RCVD state.
Curr Estab	This counter displays the number of TCP connections with a current state o ESTABLISHED or CLOSE- WAIT.
Estab Resets	This counter displays the number of times that the TCP connections make a transition to the CLOSED state from the ESTABLISHED state or the CLO state.
In Segs	This counter displays the total number of segments that are received, inclu that are received in error. This count only includes segments that are receiv currently established connections.
InOut Segs	This counter displays the total number of segments that are sent and the tot of segments that are received.

Counters	Counter Description
Out Segs	This counter displays the total number of segments that are sent. This c includes segments that are sent on currently established connections, bu retransmitted octets.
Passive Opens	This counter displays the number of times that TCP connections make a di to the SYN-RCVD state from the LISTEN state.
RetransSegs	This counter displays the total number of segments that are retransmitte segment contains one or more previously transmitted octets.

Thread

The Thread object provides a list of running threads on your system.

The following table contains information about the Thread counters.

Table 21: Thread

Counters	Counter Description
% CPU Time	This counter displays the threads share of the elapsed CPU time since th This counter expresses the share as a percentage of the total CPU time.
PID	This counter displays the threads leader process ID.

AXL Web Service

The AXL Web Service object provides information about the AXL Web Service running on your system. The following table contains information about the AXL Web Service counters.

Table 22: AXL Web Service

Counters	Counter Description
ThrottleCount	This counter represents the number of times Administrati restart of the Cisco AXL Web Service. Throttling occurs to process.
ThrottleState	This counter represents whether Administrative XML La value of 1 in this counter indicates that throttling is curre a write request to Unified Communications Manager thro continue to be allowed and processed while AXL throttlin at this time and all read and write requests will be proces

Ramfs

The Ramfs object provides information about the ram file system. The following table contains information on the Ramfs counters.

Table 23: Ramfs

Counters	Counter Description
FilesTotal	This counter represents the total number of files in the ram-based file syste
SpaceFree	This counter represents the amount of free data blocks in the ram-based file data storage for a filesystem. The block size specifies the size that the file s Communications Manager system, the block size is 4096 bytes.
SpaceUsed	This counter represents the amount of used data blocks in the ram-based fil data storage for a file system. The block size specifies the size that the file Communications Manager system, the block size is 4096 bytes.

Voice and Video Counters

Cisco Analog Access

The Cisco Analog Access object provides information about registered Cisco Analog Access gateways. The following table contains information about CiscoAnalog Access counters.

Table 24: Cisco Analog Access

Counters	Counter Description
OutboundBusyAttempts	This counter represents the total number of times that Unified Communication attempts a call through the analog access gateway when all ports were busy
PortsActive	This counter represents the number of ports that are currently in use (active appears active when a call is in progress on that port.
PortsOutOfService	This counter represents the number of ports that are currently out of service applies only to loop-start and ground-start trunks.

Cisco Annunciator Device

The Cisco Annunciator Device object provides information about registered Cisco annunciator devices. The following table contains information about CiscoAnnunciator counters.

Table 25: Cisco Annunciator Device

Counters	Counter Description
OutOfResources	This counter represents the total number of times that Unified Communication attempted to allocate an annunciator resource from an annunciator device a for example, because all resources were already in use.
ResourceActive	This counter represents the total number of annunciator resources that are c active (in use) for an annunciator device.

Counters	Counter Description
ResourceAvailable	This counter represents the total number of resources that are not active available to be used at the current time for the annunciator device.
ResourceTotal	This counter represents the total number of annunciator resources that a for an annunciator device.

Cisco Call Restriction

The Cisco Call Restriction object provides information about the number of failures that result due to logical partitioning policy restrictions. The following table contains information about Cisco Call Restriction counters.

Table 26: Cisco Call Restriction

Counters	Counter Description
AdHocConferenceFailures	This counter represents the number of attempts that failed to add a parti Ad Hoc Conference because the call path between the geolocation of th already in conference and the device being invited to the conference wa due to a logical partition policy.
BasicCallFailures	This counter represents the number of basic calls that have failed becau partition policy restrictions between the geolocations of the called and c A basic call is any call that does not utilize supplementary services such forward, and so on.
ForwardingFailures	This counter represents the number of attempts to forward an incoming failed because of a logical partition policy restriction between the geolo two parties involved.
LogicalPartitionFailuresTotal	This counter represents the total number of call attempts that have failed restriction of calls between geolocations of the calling and called parties. the number of failures for Transfer, AdHoc Conference, Meet-Me Confer Call Park, Shared Lines and Basic Calls.
MeetMeConferenceFailures	This counter represents the number of attempts that failed to add a parti Meet-Me conference because the call path between the geolocation of t already in conference and the device attempting to join the conference v due to a logical partition policy.
MidCallFailures	This counter represents the number of calls that have failed because of a between the geolocations of the called or connected parties after the init check.
ParkRetrievalFailures	This counter represents the number of attempts to perform a Call Park o failed because the device that was attempting to retrieve the call had a log policy restriction with the geolocation of the parked party.
PickUpFailures	This counter represents the number of attempts to perform a PickUp op failed because the device on which the pickup was being attempted had partition policy restriction with the geolocation of the calling device.

Counters	Counter Description
SharedLineFailures	This counter represents the number of attempts to use a shared line which faile the caller or callee has a logical partition policy restriction with the geoloca devices having the shared lines.
TransferFailures	This counter represents the number of call transfer attempts that failed due to of calls between the geolocation of the transferred party and the transferred d

Cisco CallManager

The CiscoCallManager object provides information about calls, applications, and devices that are registered with the Unified Communications Manager. The following table contains information about CiscoCallManager counters.

Table 27: CiscoCallManager

Counters	Counter Description
AnnunciatorOutOfResources	This counter represents the total number of times that Unified Communica Manager attempted to allocate an annunciator resource from those that are to a Unified Communications Manager when none were available.
AnnunciatorResourceActive	This counter represents the total number of annunciator resources that are in use on all annunciator devices that are registered with a Unified Commu Manager.
AnnunciatorResourceAvailable	This counter represents the total number of annunciator resources that are and are currently available.
AnnunciatorResourceTotal	This counter represents the total number of annunciator resources that are by all annunciator devices that are currently registered with Unified Comm Manager.
AuthenticatedCallsActive	This counter represents the number of authenticated calls that are currently use) on Unified Communications Manager. An authenticated call designat which all the endpoints that are participating in the call are authenticated. authenticated phone uses the Transport Layer Security (TLS) authenticate protocol signaling with Unified Communications Manager.
AuthenticatedCallsCompleted	This counter represents the number of authenticated calls that connected a subsequently disconnected through Unified Communications Manager. An authenticated call designates one in which all the endpoints that are partici the call are authenticated. An authenticated phone uses the TLS authenticat protocol signaling with Unified Communications Manager.
AuthenticatedPartiallyRegisteredPhone	This counter represents the number of partially registered, authenticated S
AuthenticatedRegisteredPhones	This counter represents the total number of authenticated phones that are r to Unified Communications Manager. An authenticated phone uses the TL authenticated Skinny protocol signaling with Unified Communications Ma

Counters	Counter Description
BRIChannelsActive	This counter represents the number of BRI voice channels that are curr active call on this Unified Communications Manager.
BRISpansInService	This counter represents the number of BRI spans that are currently ava
CallManagerHeartBeat	This counter represents the heartbeat of Unified Communications Man incremental count indicates that Unified Communications Manager is u If the count does not increment, that indicates that Unified Communicat is down.
CallsActive	This counter represents the number of voice or video streaming connec currently in use (active); in other words, the number of calls that actuall path that is connected on Unified Communications Manager.
CallsAttempted	This counter represents the total number of attempted calls. An attempt anytime that a phone goes off hook and back on hook, regardless of whe were dialed, or whether it connected to a destination. The system consi attempts during feature operations (such as transfer and conference) to calls.
CallsCompleted	This counter represents the number of calls that were actually connecte or video stream was established) through Unified Communications Ma number increases when the call terminates.
CallsInProgress	This counter represents the number of voice or video calls that are curren on Unified Communications Manager, including all active calls. When a phone that is registered with Skinny Client Control Protocol (S hook, the CallsInProgress progress counter increments. until it goes ba For Cisco Unified IP Phones 7940, and 7960 that register with SIP, the C counter increments when the dial softkey is pressed. For all other phones that are running SIP, the CallsInProgress counter i when the first digit is pressed. When all voice or video calls that are in progress are connected, the nu CallsInProgress represents the number of CallsActive. The counter dec when a phone goes back on hook.
CM_MediaTermPointsRequestsThrottled	This counter represents the total number of media termination point (M requests that have been denied due to throttling (a resource from this M allocated because, as specified by the Cisco CallManager service para and Transcoder Resource Throttling Percentage, the MTP was being u the configured throttle percentage). This counter increments each time an MTP on this Unified Communications Manager node is requested a to MTP throttling and reflects a running total since the start of the Cisco Service.

Performance Counters and Alerts

Counters	Counter Description
CM_TranscoderRequestsThrottled	This counter represents the total number of transcoder resource requests th been denied due to throttling (a resource from this transcoder was not allocate as specified by the Cisco CallManager service parameter MTP and Transc Resource Throttling Percentage, the transcoder was being utilized beyond configured throttle percentage). This counter increments each time a reque transcoder on this Unified Communications Manager node is requested an due to transcoder throttling and reflects a running total since the start of th CallManager Service.
EncryptedCallsActive	This counter represents the number of encrypted calls that are currently acti on this Unified Communications Manager. An encrypted call represents on all the endpoints that are participating in the call are encrypted.
EncryptedCallsCompleted	This counter represents the number of encrypted calls that were connected subsequently disconnected through this Unified Communications Manage encrypted call represents one in which all the endpoints that are participati call are encrypted.
EncryptedPartiallyRegisteredPhones	This counter represents the number of partially registered, encrypted SIP p
EncryptedRegisteredPhones	This counter represents the total number of encrypted phones that are regis this Unified Communications Manager.
FXOPortsActive	This counter represents the number of FXO ports that are currently in use (a Unified Communications Manager.
FXOPortsInService	This counter represents the number of FXO ports that are currently availab in the system.
FXSPortsActive	This counter represents the number of FXS ports that are currently in use (a Unified Communications Manager.
FXSPortsInService	This counter represents the number of FXS ports that are currently availab in the system.
HuntListsInService	This counter represents the number of hunt lists that are currently in service Communications Manager.
HWConferenceActive	This counter represents the total number of hardware conference resources provided by all hardware conference bridge devices that are currently regis Unified Communications Manager.
HWConferenceCompleted	This counter represents the total number of conferences that used a hardware bridge (hardware-based conference devices such as Cisco Catalyst 6000, Cisc 4000, Cisco VG200, Cisco series 26xx and 36xx) that is allocated from Un Communications Manager and that have completed, which means that the bridge has been allocated and released. A conference activates when the fi connects to the bridge. The conference completes when the last call disconn the bridge.

Counters	Counter Description
HWConferenceOutOfResources	This counter represents the total number of times that Unified Commu Manager attempted to allocate a hardware conference resource from th registered to a Unified Communications Manager when none was avai
HWConferenceResourceActive	This counter represents the total number of conference resources that ar hardware conference devices (such as Cisco Catalyst 6000, Catalyst 40 VG200, Cisco series 26xx and 36xx) that are registered with Unified Co Manager. System considers conference to be active when one or more connected to a bridge.
HWConferenceResourceAvailable	This counter represents the number of hardware conference resources t use and that are available to be allocated on all hardware conference de Cisco Catalyst 6000, Cisco Catalyst 4000, Cisco VG200, Cisco series 2 that are allocated from Unified Communications Manager and that hav completed, which means that the conference bridge has been allocated A conference activates when the first call connects to the bridge. The c completes when the last call disconnects from the bridge.
HWConferenceResourceTotal	This counter represents the number of active conferences on all hardwa devices that are registered with Unified Communications Manager.
InitializationState	This counter represents the current initialization state of Unified Comm Manager. Unified Communications Manager includes the following initi values: 1-Database, 2-Regions, 3-Locations, 4-QoS Policy, 5-Time Of Day, 6- Neighborhoods, 7-Digit Analysis, 8-Route Plan, 9-Call Control, 10-RS Manager, 11-Supplementary Services, 12-Directory, 13-SDL Link, 14- 100-Initialization Complete. Not all states display when this counter is used. This display does not in error occurred; this display simply indicates that the states initialized a within the refresh period of the performance monitor.
IVRResourceActive	This represents the total number of IVR resources that are currently in u devices registered with Unified Communications Manager.
IVROutOfResources	This represents the total number of times Unified Communications Mana to allocate an IVR resource from those that are registered to Unified Co Manager when none were available.
IVRResourceAvailable	This represents the total number of IVR resources provided by all IVR are currently registered with Unified Communications Manager.
IVRResourceTotal	This represents the total number of IVR resources provided by all IVR are currently registered with Unified Communications Manager.
LocationOutOfResources	This counter represents the total number of times that a call through Lo due to the lack of bandwidth.

Counters	Counter Description
MCUConferencesActive	This counter represents the total number of active conferences on all Cisco TelePresence MCU conference bridge devices that are registered with Uni Communications Manager.
MCUConferencesCompleted	This counter represents the total number of conferences that used a Cisco Tel MCU conference bridge allocated from Unified Communications Manage completed, implying that the conference bridge was allocated and released conference is activated when the first call is connected to the bridge. The c is completed when the last call is disconnected from the bridge.
MCUHttpConnectionErrors	This counter represents the total number of times Unified Communications attempted to create HTTP connections to Cisco TelePresence MCU confere device, and failed due to connection errors on the Cisco TelePresence MCU c bridge side.
MCUHttpNon200OKResponse	This counter represents the total number of times Unified Communications received a non 200 OK HTTP Response from Cisco TelePresence MCU co bridge, for any HTTP query sent.
MCUOutOfResources	This counter represents the total number of times Unified Communications attempted to allocate a conference resource from Cisco TelePresence MCU c bridge device and failed. For example, the attempt to allocate a conference fails, if all the resources are already in use.
MOHMulticastResourceActive	This counter represents the total number of multicast Music On Hold (MOH) that are currently in use (active) on all MOH servers that are registered with Communications Manager.
MOHMulticastResourceAvailable	This counter represents the total number of active multicast MOH connect are not being used on all MOH servers that are registered with a Unified Communications Manager.
MOHOutOfResources	This counter represents the total number of times that the Media Resource attempted to allocate an MOH resource when all available resources on all servers that are registered with a Unified Communications Manager were a active.
MOHTotalMulticastResources	This counter represents the total number of multicast MOH resources or co that are provided by all MOH servers that are currently registered with a U Communications Manager.
MOHTotalUnicastResources	This counter represents the total number of unicast MOH resources or stre are provided by all MOH servers that are currently registered with Unified Communications Manager. Each MOH unicast resource uses one stream.
MOHUnicastResourceActive	This counter represents the total number of unicast MOH resources that are in use (active) on all MOH servers that are registered with Unified Commu Manager. Each MOH unicast resource uses one stream.

Counters	Counter Description
MOHUnicastResourceAvailable	This counter represents the total number of unicast MOH resources tha available on all MOH servers that are registered with Unified Commur Manager. Each MOH unicast resource uses one stream.
MTPOutOfResources	This counter represents the total number of times that Unified Commu Manager attempted but failed to allocate a media termination point (M from one MTP device that is registered with Unified Communications M also means that no transcoders were available to act as MTPs.
MTPResourceActive	This counter represents the total number of MTP resources that are cur (active) on all MTP devices that are registered with a Unified Commur Manager. Each MTP resource uses two streams. An MTP in use repres resource that has been allocated for use in a call.
MTPResourceAvailable	This counter represents the total number of MTP resources that are not available to be allocated on all MTP devices that are registered with U Communications Manager. Each MTP resource uses two streams. An M represents one MTP resource that has been allocated for use in a call.
MTPResourceTotal	This counter represents the total number of MTP resources that are pro MTP devices that are currently registered with Unified Communicatio
MTP_RequestsThrottled	This counter represents the total number of MTP resource requests tha denied due to throttling (a resource from this MTP was not allocated b specified by the Cisco CallManager service parameter MTP and Transc Throttling Percentage, the MTP was being utilized beyond the configu percentage). This counter increments each time a resource is requested f and is denied due to throttling. This counter reflects a running total sin device registered with the Cisco CallManager Service.
PartiallyRegisteredPhone	This counter represents the number of partially registered phones that ar
PRIChannelsActive	This counter represents the number of PRI voice channels that are in an a Unified Communications Manager.
PRISpansInService	This counter represents the number of PRI spans that are currently ava
RegisteredAnalogAccess	This counter represents the number of registered Cisco analog access g are registered with system. The count does not include the number of C access ports.
RegisteredHardwarePhones	This counter represents the number of Cisco hardware IP phones (for ex Unified IP Phones 7960, 7940, and so on.) that are currently registered
RegisteredMGCPGateway	This counter represents the number of MGCP gateways that are curren in the system.
RegisteredOtherStationDevices	This counter represents the number of station devices other than Cisco phones that are currently registered in the system (for example, Cisco I CTI port, CTI route point, Cisco voicemail port).

Counters	Counter Description
RegisteredTCTJabberNonMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Cisco Jabber on iPhone devices that are cur registered on-premise in the system.
RegisteredTCTJabberMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Cisco Jabber on iPhone devices that are cur registered in the system over Mobile and Remote Access.
RegisteredBOTJabberNonMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Cisco Jabber on Android devices that are cu registered on-premise in the system.
RegisteredBOTJabberMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Cisco Jabber on Android devices that are cu registered in the system over Mobile and Remote Access.
RegisteredTABJabberNonMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Cisco Jabber on iPad devices that are currently on-premise in the system.
RegisteredTABJabberMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Cisco Jabber on iPad devices that are currently in the system over Mobile and Remote Access.
RegisteredCSFJabberNonMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Cisco Jabber on desktop devices that are cu registered on-premise in the system.
RegisteredCSFJabberMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Cisco Jabber on desktop devices that are cu registered in the system over Mobile and Remote Access.
RegisteredTCTWebexNonMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Webex App on iPhone devices that are curr registered on-premise in the system.
RegisteredTCTWebexMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Webex App on iPhone devices that are curr registered in the system over Mobile and Remote Access.
RegisteredBOTWebexNonMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Webex App on Android devices that are cur registered on-premise in the system.

Counters	Counter Description
RegisteredBOTWebexMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Webex App on Android devices that are registered in the system over Mobile and Remote Access.
RegisteredTABWebexNonMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Webex App on iPad devices that are curre on-premise in the system.
RegisteredTABWebexMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Webex App on iPad devices that are curre in the system over Mobile and Remote Access.
RegisteredCSFWebexNonMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Webex App on desktop devices that are registered on-premise in the system.
RegisteredCSFWebexMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Webex App on desktop devices that are registered in the system over Mobile and Remote Access.
RegisteredHardwarePhonesMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Cisco hardware IP phones (for example, 7841, 8845, 8865, and so on.) that are currently registered in the systen and Remote Access.
RegisteredDualModeDevices **Important** Applicable from Release 14SU1 onwards.	This counter details the dual-mode devices that are registered over Mobi Access and on-premise. TCT and BOT are the only dual-mode devices
RegisteredDevicesMRA **Important** Applicable from Release 14SU1 onwards.	This represents the number of Cisco IP Phones and Dual-mode devices currently registered in the system over Mobile and Remote Access.
SIPLineServerAuthorizationChallenges	This counter represents the number of authentication challenges for inc requests that the Unified Communications Manager server issued to ph running SIP. An authentication challenge occurs when a phone that is r with Digest Authentication enabled sends a SIP line request to Unified Co Manager.
SIPLineServerAuthorizationFailures	This counter represents the number of authentication challenge failures SIP requests from SIP phones to the Unified Communications Manage authentication failure occurs when a SIP phone with Digest Authentica sends a SIP line request with bad credentials to Unified Communicatio

Performance Counters and Alerts

Counters	Counter Description
SIPTrunkAuthorization	This counter represents the number of application-level authorization chec incoming SIP requests that Unified Communications Manager has issued to S An application-level authorization check occurs when Unified Communica Manager compares an incoming SIP request to the application-level setting SIP Trunk Security Profile Configuration window in Cisco Unified Comm Manager Administration.
SIPTrunkAuthorizationFailures	This counter represents the number of application-level authorization failu incoming SIP requests that have occurred on Unified Communications Ma trunks. An application-level authorization failure occurs when Unified Comm Manager compares an incoming SIP request to the application-level autho settings on the SIP Trunk Security Profile Configuration window in Cisco Communications Manager Administration and finds that authorization for o of the SIP features on that window is not allowed.
SIPTrunkServerAuthenticationChallenges	This counter represents the number of authentication challenges for incom requests that Unified Communications Manager issued to SIP trunks. An auth challenge occurs when a SIP trunk with Digest Authentication enabled ser request to Unified Communications Manager.
SIPTrunkServerAuthenticationFailures	This counter represents the number of authentication challenge failures tha for incoming SIP requests from SIP trunks to Unified Communications Ma authentication failure occurs when a SIP trunk with Digest Authentication sends a SIP request with bad credentials to Unified Communications Mana
SWConferenceActive	This counter represents the number of active conferences on all software c devices that are registered with Unified Communications Manager.
SWConferenceCompleted	This counter represents the total number of conferences that used a software c bridge that was allocated from a Unified Communications Manager and th been completed, which means that the conference bridge has been allocate released. A conference activates when the first call connects to the bridge. conference completes when the last call disconnects from the bridge.
SWConferenceOutOfResources	This counter represents the total number of times that Unified Communica Manager attempted to allocate a software conference resource from those registered to Unified Communications Manager when none were available includes failed attempts to add a new participant to an existing conference
SWConferenceResourceActive	This counter represents the total number of conference resources that are in software conference devices that are registered with Unified Communications The system considers a conference to be active when one or more calls co bridge. One resource equals one stream.
SWConferenceResourceAvailable	This counter represents the number of new software-based conferences tha started at the same time, for Unified Communications Manager. You must minimum of three streams available for each new conference. One resourc one stream.

Counters	Counter Description
SWConferenceResourceTotal	This counter represents the total number of software conference resour provided by all software conference bridge devices that are currently r Unified Communications Manager.
SystemCallsAttempted	This counter represents the total number of server-originated calls and a to the Unity message waiting indicator (MWI).
T1ChannelsActive	This counter represents the number of T1 CAS voice channels that are call on a Unified Communications Manager.
T1SpansInService	This counter represents the number of T1 CAS spans that are currently use.
TLSConnectedSIPTrunks	This counter represents the number of SIP trunks that are configured a through Transport Layer Security (TLS).
TLSConnectedWSM	This counter represents the number of WSM Connectors that is config connected to Motorola WSM through Transport Layer Security (TLS).
TranscoderOutOfResources	This counter represents the total number of times that Unified Commu Manager attempted to allocate a transcoder resource from a transcoder registered to a Unified Communications Manager when none was avai
TranscoderResourceActive	This counter represents the total number of transcoders that are in use on devices that are registered with Unified Communications Manager. A t use represents one transcoder resource that has been allocated for use i transcoder resource uses two streams.
TranscoderResourceAvailable	This counter represents the total number of transcoders that are not in us available to be allocated on all transcoder devices that are registered w Communications Manager. Each transcoder resource uses two streams
TranscoderResourceTotal	This counter represents the total number of transcoder resources that ar all transcoder devices that are currently registered with Unified Comm Manager.
VCBConferenceActive	This counter represents the total number of active video conferences o conference bridge devices that are registered with Unified Communicat
VCBConferenceAvailable	This counter represents the total number of new video conferences on a conference bridge devices that are registered with Unified Communicat
VCBConferenceCompleted	This counter represents the total number of video conferences that use conference bridge that is allocated from Unified Communications Man have been completed, which means that the conference bridge has been released. A conference activates when the first call connects to the brid conference completes when the last call disconnects from the bridge.
VCBConferenceTotal	This counter represents the total number of video conferences that are all video conference bridge devices that are registered with Unified Co Manager.

Counters	Counter Description
VCBOutOfConferences	This counter represents the total number of times that Unified Communica Manager attempted to allocate a video conference resource from those tha registered to Unified Communications Manager when none was available.
VCBOutOfResources	This counter represents the total number of failed new video conference re conference request can fail because, for example, the configured number of c is already in use.
VCBResourceActive	This counter represents the total number of video conference resources that ar in use on all video conference devices that are registered with Unified Comm Manager.
VCBResourceAvailable	This counter represents the total number of video conference resources tha active and are currently available.
VCBResourceTotal	This counter represents the total number of video conference resources that ar by all video conference bridge devices that are currently registered with U Communications Manager.
VideoCallsActive	This counter represents the number of active video calls with active video connections on all video conference bridge devices that are registered with Communications Manager.
VideoCallsCompleted	This counter represents the number of video calls that were actually conne video streams and then released.
VideoOutOfResources	This counter represents the total number of times that Unified Communica Manager attempted to allocate a video-streaming resource from one of the conference bridge devices that is registered to Unified Communications M when none was available.
XCODE_RequestsThrottled	This counter represents the total number of transcoder resource requests th been denied due to throttling (a resource from this transcoder was not allocate as specified by the Cisco CallManager service parameter MTP and Transc Resource Throttling Percentage, the transcoder was being utilized beyond configured throttle percentage). This counter increments each time a resou requested from this transcoder and is denied due to throttling. This counter running total since the transcoder device registered with the Cisco CallManag

Cisco CallManager System Performance

The CiscoCallManager System Performance object provides system performance information about Unified Communications Manager. The following table contains information about CiscoCallManager system performance counters.

Table 28: CiscoCallManager System Performance

Counters	Counter Description
AverageExpectedDelay	This counter represents the current average expected delay before any inco gets handled.
CallsRejectedDueToICTThrottling	This counter represents the total number of calls that were rejected sinc CiscoCallManager service due to Intercluster Trunk (ICT) call throttlin threshold limit of 140 calls per 5 seconds is met, the ICT will start throttli new calls. One cause for ICT call throttling occurs when calls across an route loop condition.
CallThrottlingGenericCounter3	This counter represents a generic counter that is used for call-throttling
CodeRedEntryExit	This counter indicates whether Unified Communications Manager has ent a Code state (call-throttling mode). Valid values include 0 (Exit) and 1 (
CodeYellowEntryExit	This counter indicates whether Unified Communications Manager has ent a Code Yellow state (call-throttling mode). Valid values include 0 (Exit)
EngineeringCounter1	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter2	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter3	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter4	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter5	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter6	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter7	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter8	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
QueueSignalsPresent 1-High	This counter indicates the number of high-priority signals in the Unifie Communications Manager queue. High-priority signals include timeout e Unified Communications Manager keepalives, certain gatekeeper event process creation, among other events. A large number of high-priority e cause degraded performance on Unified Communications Manager and call connection or loss of dial tone. Use this counter in conjunction wit QueueSignalsProcessed 1-High counter to determine the processing del Communications Manager.

Counters	Counter Description
QueueSignalsPresent 2-Normal	This counter indicates the number of normal-priority signals in the Unified Communications Manager queue. Normal-priority signals include call-proc functions, key presses, on-hook and off-hook notifications, among other ev large number of normal-priority events will cause degraded performance o Communications Manager, sometimes resulting in delayed dial tone, slow connection, or loss of dial tone. Use this counter in conjunction with the QueueSignalsProcessed 2-Normal counter to determine the call-processing Unified Communications Manager. Remember that high-priority signals mus before normal-priority signals begin to process, so check the high-priority c well to get an accurate picture of the potential delay.
QueueSignalsPresent 3-Low	This counter indicates the number of low-priority signals in the Unified Comm Manager queue. Low-priority signals include station device registration (ex initial station registration request message), among other events. A large nu signals in this queue could result in delayed device registration, among oth
QueueSignalsPresent 4-Lowest	This counter indicates the number of lowest priority signals in the Unified Communications Manager queue. Lowest priority signals include the initia registration request message during device registration, among other events number of signals in this queue could result in delayed device registration, other events.
QueueSignalsProcessed 1-High	This counter indicates the number of high-priority signals that Unified Comm Manager processes for each 1-second interval. Use this counter in conjunct the QueueSignalsPresent 1-High counter to determine the processing delay queue.
QueueSignalsProcessed 2-Normal	This counter indicates the number of normal-priority signals that Unified Communications Manager processes for each 1-second interval. Use this co conjunction with the QueueSignalsPresent 2-Normal counter to determine the delay on this queue. Remember that high-priority signals get processed bef normal-priority signals.
QueueSignalsProcessed 3-Low	This counter indicates the number of low-priority signals that Unified Comm Manager processes for each 1-second interval. Use this counter in conjunct the QueueSignalsPresent 3-Low counter to determine the processing delay queue. The number of signals processed gives an indication of how much d registration activity is being processed in this time interval.
QueueSignalsProcessed 4-Lowest	This counter indicates the number of lowest priority signals that Unified Communications Manager processes for each 1-second interval. Use this co conjunction with the QueueSignalsPresent 4-Lowest counter to determine the delay on this queue. The number of signals that are processed gives an indi how many devices began the Unified Communications Manager registratio in this time interval.
QueueSignalsProcessed Total	This counter provides a sum total of all queue signals that Unified Commu Manager processes for each 1-second period for all queue levels: high, nor and lowest.

Counters	Counter Description
SkinnyDevicesThrottled	This counter represents the total number of Skinny devices that are bein Skinny device gets throttled (asked to shut down and reregister) when the of events that the Skinny device generated exceeds the configured maxim value (default value specifies 2000 events) within a 5-second interval.
ThrottlingSampleActivity	This counter indicates how many samples, out of the configured sample non-zero averageExpectedDelay values. This counter resets when any s averageExpectedDelay value of zero. This process repeats for each batc A batch represents the configured sample size.
TotalCodeYellowEntry	This counter indicates the number of times that Unified Communication call processing enters the code yellow state. This counter remains cumul start of the Unified Communications Manager process.

Cisco CTIManager

The Cisco CTI Manager object provides information about Cisco CTI Manager. The following table contains information about CiscoCTIManager counters.

Table 29: Cisco CTI Manager

Counters	Counter Description
CcmLinkActive	This counter represents the total number of active Unified Communicat links. CTI Manager maintains links to all active servers in a cluster, if a
CTIConnectionActive	This counter represents the total number of CTI clients that are currently the CTIManager. This counter increases by one when new connection i and decreases by one when a connection is released. The CTIManager serv MaxCTIConnections determines the maximum number of active conne
DevicesOpen	This counter represents the total number of devices that are configured Communications Manager that CTI applications control and/or monitor include hardware IP phones, CTI ports, CTI route points, and so on.
LinesOpen	This counter represents the total number of lines that are configured in Communications Manager that control and/or monitor CTI applications
QbeVersion	This counter represents the version number of the Quick Buffer Encodi interface that the CTIManager uses.

Cisco Dual-Mode Mobility

The Cisco Dual-Mode Mobility object provides information about the dual-mode mobility application on Unified Communications Manager. The following table contains information about CiscoDual-Mode Mobility counters.

Table 30: Cisco Dual-Mode Mobility

Counters	Counter Description
CallsAnchored	This counter represents the number of calls that are placed or received on d phones that are anchored in Unified Communications Manager. The counter i when a call is received from or placed to a dual-mode phone. The counter i twice if a dual-mode phone calls another dual-mode phone.
DMMSRegistered	This counter represents the number of Dual-mode Mobile Station (DMMS) s that are registered in the wireless LAN (WLAN).
FollowMeAborted	This counter represents the number of failed follow-me operations.
FollowMeAttempted	This counter represents the number of follow-me operations that Unified Communications Manager attempted. The counter increments when a SIP 30 Temporarily message is received from the Wireless Service Manager (WSM Unified Communications Manager redirects the call to the DMMS in WLA
FollowMeCompleted	This counter represents the number of follow-me operations that were succ completed. The counter increments when the DMMS in WLAN answers th the media (voice path) is successfully established with the calling device.
FollowMeInProgress	This counter represents the number of follow-me operations that are curren progress. The counter increments when a follow-me is attempted, and it de when the follow-me operation is aborted or completed.
H1HandOutAttempted	This counter represents the number of H1 hand-out operations that dual-mo attempt. The counter increments when Unified Communications Manager p a call to the H1 number from a DMMS.
H1HandOutCompleted	This counter represents the number of successfully completed H1 hand-out o The counter increments when the DMMS in WLAN successfully reestablish (voice path).
H2HandOutCompleted	This counter represents the number of successfully completed H2 hand-out o The counter increments when the DMMS in WLAN successfully reestablish (voice path).
H2HandOutsAttempted	This counter represents the number of H2 hand-out operations that dual-mo attempt. The counter increments when Unified Communications Manager r call to the H2 number from a DMMS.
HandInAborted	This counter represents the number of hand-in operations that failed.
HandInAttempted	This counter represents the number of hand-in operations that dual-mode p attempt.
HandInCompleted	This counter represents the number of successfully completed hand-in opera counter increments when the DMMS in WLAN successfully reestablishes a (voice path).

Counters	Counter Description
HandInInProgress	This counter represents the number of hand-in operations that are current The counter increments when a hand-in is attempted, and the counter dec the hand-in is aborted or completed.
HandOutAborted	This counter represents the number of hand-out operations that failed.
HandOutInProgress	This counter represents the number of H1 and H2 hand-out operations tha in progress. The counter increments when a H1 or H2 hand-out is attem decrements when the hand-out is aborted or completed.

Cisco Extension Mobility

The Cisco Extension Mobility object provides information about the extension mobility application. The following table contains information about Cisco Extension Mobility counters.

Table 31: Cisco Extension Mobility Application

Counters	Counter Description
RequestsHandled	This counter represents the total number of HTTP requests that the exter application handled since the last restart of the CiscoCallManager servi login would constitute two HTTP requests: one to query the initial logi device and another to log in the user on a device. Similarly, a typical logo in two HTTP requests.
RequestsInProgress	This counter represents the number of HTTP requests that the extensior application currently is handling. A typical login would constitute two H one to query the initial login state of the device and another to log in th device. Similarly, a typical logout also results in two HTTP requests.
RequestsThrottled	This counter represents the total number of Login/Logout Requests that throttling.
LoginsSuccessful	This counter represents the total number of successful login requests th completed through EM Service.
LogoutsSuccessful	This counter represents the total number of successful logout requests t completed through EM Service
Total Login/LogoutRequestsAttempted	This counter represents the total number of Login and Logout requests attempted through this EM Service. This number includes both success unsuccessful attempts.

Cisco Gatekeeper

The Cisco Gatekeeper object provides information about registered Cisco gatekeeper devices. The following table contains information about Ciscogatekeeper device counters.

Table 32: Cisco Gatekeeper

Counters	Counter Description
ACFsReceived	This counter represents the total number of RAS Admission Confirm messa are received from the configured gatekeeper and its alternate gatekeepers.
ARQsAttempted	This counter represents the total number of RAS Admission Request messa are attempted by using the configured gatekeeper and its alternate gatekeep
RasRetries	This counter represents the number of retries due to loss or delay of all RA acknowledgement messages on the configured gatekeeper and its alternate ga
VideoOutOfResources	This counter represents the total number of video-stream requests to the co gatekeeper or its alternate gatekeepers that failed, most likely due to lack of b

Cisco H.323

The Cisco H.323 object provides information about registered Cisco H.323 devices. The following table contains information about Cisco H.323 device counters.

Table 33: Cisco H.323

Counters	Counter Description
CallsActive	This counter represents the number of streaming connections that are curre (in use) on the configured H.323 device; in other words, the number of call actually have a voice path that is connected.
CallsAttempted	This counter represents the total number of calls that have been attempted o including both successful and unsuccessful call attempts.
CallsCompleted	This counter represents the total number of successful calls that were made device.
CallsInProgress	This counter represents the number of calls that are currently in progress o
CallsRejectedDueToICTCallThrottling	This counter represents the total number of calls rejected due to Intercluste (ICT) call throttling since the start of the CiscoCallManager service. When t reaches a threshold limit of 140 calls per 5 seconds, ICT will start throttling new calls. One cause for ICT call throttling occurs when calls across an IC route loop condition.
VideoCallsActive	This counter represents the number of video calls with video streaming co that are currently active (in use) on all H.323 trunks that are registered with Communications Manager; in other words, the number of calls that actuall video-streaming connections on a Unified Communications Manager.
VideoCallsCompleted	This counter represents the number of video calls that were actually connec video streams for all H.323 trunks that were registered with a Unified Comm Manager. This number increases when the call terminates.

Cisco Hunt Lists

The Cisco Hunt Lists object provides information about the hunt lists that are defined in Cisco Unified Communications Manager Administration. The following table contains information about Cisco hunt list counters.

Table 34: Cisco Hunt Lists

Counters	Counter Description
CallsAbandoned	This counter represents the number of abandoned calls that occurred thr list. An abandoned call represents one in which a caller hangs up before answered.
CallsActive	This counter represents the number of calls that are currently active (in occurred through a hunt list. An active call represents one that gets distr answered, and to which a voice path connects.
CallsBusyAttempts	This counter represents the number of times that calls through a hunt list w when all members of the line and/or route groups were busy.
CallsInProgress	This counter represents the number of calls that are currently in progres hunt list. A call in progress represents one that the call distributor is atte extend to a member of a line or route group and that has not yet been an Examples of a hunt list member include a line, a station device, a trunk port/channel of a trunk device.
CallsRingNoAnswer	This counter represents the total number of calls through a hunt list that called parties did not answer.
HuntListInService	This counter specifies whether the particular hunt list is currently in ser of 0 indicates that the hunt list is out of service; a value of 1 indicates tha is in service. Reasons that a hunt list could be out of service include the l running on a primary Unified Communications Manager based on its U Communications Manager Group or the hunt list has been disabled in C Communications Manager Administration.
MembersAvailable	This counter represents the total number of available or idle members of groups that belong to an in-service hunt list. An available member curre a call and will accept a new call. An idle member does not handle any c accept a new call. A hunt list member can comprise a route group, line combination. A member of a line group represents a directory number o IP phone or a voice-mail port. A member of a route group represents a sta a trunk gateway, or port/channel of a trunk gateway.

Cisco HW Conference Bridge Device

The Cisco HW Conference Bridge Device object provides information about registered Cisco hardware conference bridge devices. The following table contains information about Cisco hardware conference bridge device counters.

Table 35: Cisco HW Conference Bridge Device

Counters	Counter Description
HWConferenceActive	This counter represents the number of conferences that are currently active (a HW conference bridge device. One resource represents one stream.
HWConferenceCompleted	This counter represents the total number of conferences that have been allo released on a HW conference device. A conference starts when the first cal to the bridge. The conference completes when the last call disconnects from t
OutOfResources	This counter represents the total number of times that an attempt was made t a conference resource from a HW conference device and failed, for exampl all resources were already in use.
ResourceActive	This counter represents the number of resources that are currently in use (a this HW conference device. One resource represents one stream.
ResourceAvailable	This counter represents the total number of resources that are not active an available to be used now for a HW conference device. One resource repres stream.
ResourceTotal	This counter represents the total number of resources for a HW conference device. This counter equals the sum of the counters ResourceAvailable and ResourceActive. One resource represents one stream.

Cisco IP Manager Assistant

The Cisco IP Manager Assistant (IPMA) Service object provides information about the Cisco Unified Communications Manager Assistant application. The following table contains information on Cisco IPMA counters.

Table 36: Cisco IP Manager Assistant Service

Counters	Counter Description
AssistantsActive	This counter represents the number of assistant consoles that are currently a active assistant console exists when an assistant is logged in from the assista desktop application.
LinesOpen	This counter represents the number of phone lines that the Cisco Unified Communications Manager Assistant application opened. An open phone li when the application assumes line control from CTI.
ManagersActive	This counter represents the current number of managers that the Cisco IPM servicing.
SessionsCurrent	This counter represents the total number of managers assistants that are curre the Cisco Unified Communications Manager Assistant application. Each ma each assistant constitute an active session; so, for one manager/assistant pa counter would reflect two sessions.

Cisco LBM service

The Cisco LBM service object provides information about LBM service that is defined in Unified Communications Manager. The following table contains information on Cisco LBM service counters.

Table 37: Cisco LBM service

Counters	Counter Description
Is Hub[1] or Spoke[0]	This counter represents the state of Location Bandwidth Manager is represented by 0 and hub state with a value of 1.
LocalHubNodesConnected	This counter represents the number of local hub nodes connected.
LocalSpokesNodesConnected	This counter represents the number of local spoke nodes connecte
RemoteHubNodesConnectedInsecure	This counter represents the number of insecure remote hub nodes
RemoteHubNodesConnectedSecure	This counter represents the number of secure remote hub nodes c

Cisco Lines

The Cisco Lines object represents the number of Cisco lines (directory numbers) that can dial and connect to a device. Lines represent all directory numbers that terminate on an endpoint. The directory number that is assigned to it identifies the line. The Cisco Lines object does not include directory numbers that include wildcards such as a pattern for a Digital or Analog Access gateway.

The Active counter represents the state of the line, either active or not active. A zero indicates that the line is not in use. When the number is greater than zero, this indicates that the line is active, and the number represents the number of calls that are currently in progress on that line. If more than one call is active, this indicates that the call is on hold either because of being placed on hold specifically (user hold) or because of a network hold operation (for example, a transfer is in progress, and it is on transfer hold). This applies to all directory numbers that are assigned to any device.

Cisco Locations LBM

The Cisco Location LBM object provides information about locations that are defined in Unified Communications Manager clusters. The following table contains information on Cisco location counters.

Table 38: Cisco Locations LBM

Counters	Counter Description
BandwidthAvailable	This counter represents the current audio bandwidth in a link between two locations. A value of 0 indicates th bandwidth is available.
BandwidthMaximum	This counter represents the maximum audio bandwidth th in a location or a link between two locations. A value o that no audio bandwidth is available.

Counters	Counter Description
BandwidthOversubscription	This represents the current oversubscribed audio bandwidt location or link between two locations. A value of zero inc bandwidth oversubscription.
CallsInProgress	This counter represents the number of calls that are curren progress on a particular Cisco Location Bandwidth Manag
ImmersiveOutOfResources	This represents the total number of failed immersive video bandwidth reservations associated with a location or a link two locations due to lack of immersive video bandwidth.
ImmersiveVideoBandwidthAvailable	This counter represents the maximum bandwidth that is av video in a location or a link between two locations. A valu indicates that no bandwidth is allocated for video.
ImmersiveVideoBandwidthMaximum	This counter represents the bandwidth that is currently ava video in a location or a link between two locations. A valu indicates that no bandwidth is available.
ImmersiveVideoBandwidthOversubscription	This represents the current immersive video oversubscribed b in a location or link between two locations. A value of zero no bandwidth oversubscription.
OutOfResources	This counter represents the total number of failed audio call b reservations associated with a given location or a link betw locations due to lack of audio bandwidth.
VideoBandwidthAvailable	This counter represents the bandwidth that is currently ava video in a location or a link between two locations. A valu indicates that no bandwidth is available.
VideoBandwidthMaximum	This counter represents the maximum bandwidth that is av video in a location and a link between two locations. A va indicates that no bandwidth is allocated for video.
VideoOversubscription	This represents the current video oversubscribed bandwidt in a location and a link between two locations. A value of indicates no bandwidth oversubscription.
VideoOutOfResources	This counter represents the total number of failed video call b reservations associated with a given location or a link betw locations due to lack of video bandwidth.

Cisco Locations RSVP

The Cisco Location RSVP object provides information about RSVP that is defined in Unified Communications Manager. The following table contains information on Cisco location RSVP counters.

Table 39: Cisco Locations RSVP

Counters	Counter Description
RSVP AudioReservationErrorCounts	This counter represents the number of RSVP reservation errors in the a
RSVP MandatoryConnectionsInProgress	This counter represents the number of connections with mandatory RSV progress.
RSVP OptionalConnectionsInProgress	This counter represents the number of connections with optional RSVP progress.
RSVP TotalCallsFailed	This counter represents the number of total calls that failed due to a RSV failure.
RSVP VideoCallsFailed	This counter represents the number of video calls that failed due to a RSV failure.
RSVP VideoReservationErrorCounts	This counter represents the number of RSVP reservation errors in the v

Cisco Media Streaming Application

The Cisco IP Voice Media Streaming Application object provides information about the registered MTPs, MOH servers, conference bridge servers, and annunciators. The following table contains information on Cisco IP Voice Media Streaming Application counters.

Note One object exists for each Unified Communications Manager in the Unified Communications Manager group that is associated with the device pool that the annunciator device is configured to use.

Table 40: Cisco Media Streaming Application

Counter	Counter Description
ANNConnectionsLost	This counter represents the total number of times since the last restart o Voice Media Streaming Application that a Unified Communications Ma connection was lost.
ANNConnectionState	For each Unified Communications Manager that is associated with an a this counter represents the current registration state to Unified Commun Manager; 0 indicates no registration to Unified Communications Manag registration to the primary Unified Communications Manager; 2 indicat to the secondary Unified Communications Manager (connected to Unif Communications Manager but not registered until the primary Unified Co Manager connection fails).
ANNConnectionsTotal	This counter represents the total number of annunciator instances that hav since the Cisco IP Voice Media Streaming Application service started.
ANNInstancesActive	This counter represents the number of actively playing (currently in use announcements.

Counter	Counter Description
ANNStreamsActive	This counter represents the total number of currently active simplex (one d streams for all connections. Each stream direction counts as one stream. On stream provides the audio input and another output stream to the endpoint c
ANNStreamsAvailable	This counter represents the remaining number of streams that are allocated annunciator device that are available for use. This counter starts as 2 multipl number of configured connections (defined in the Cisco IP Voice Media St App service parameter for the Annunciator, Call Count) and is reduced by on active stream that started.
ANNStreamsTotal	This counter represents the total number of simplex (one direction) streams connected to the annunciator device since the Cisco IP Voice Media Stream Application service started.
CFBConferencesActive	This counter represents the number of active (currently in use) conferences
CFBConferencesTotal	This counter represents the total number of conferences that started since th Voice Media Streaming Application service started.
CFBConnectionsLost	This counter represents the total number of times since the last restart of th Voice Media Streaming Application that a Unified Communications Manag connection was lost.
CFBConnectionState	For each Unified Communications Manager that is associated with a SW C Bridge, this counter represents the current registration state to Unified Comm Manager; 0 indicates no registration to Unified Communications Manager; 1 registration to the primary Unified Communications Manager; 2 indicates c to the secondary Unified Communications Manager (connected to Unified Communications Manager but not registered until the primary Unified Comm Manager connection fails).
CFBStreamsActive	This counter represents the total number of currently active simplex (one d streams for all conferences. Each stream direction counts as one stream. In a t conference, the number of active streams equals 6.
CFBStreamsAvailable	This counter represents the remaining number of streams that are allocated conference bridge that are available for use. This counter starts as 2 multipl number of configured connections (defined in the Cisco IP Voice Media St App service parameter for Conference Bridge, Call Count) and is reduced b each active stream started.
CFBStreamsTotal	This counter represents the total number of simplex (one direction) streams connected to the conference bridge since the Cisco IP Voice Media Streami Application service started.

Counter	Counter Description
MOHAudioSourcesActive	This counter represents the number of active (currently in use) audio so MOH server. Some of these audio sources may not be actively streamin if no devices are listening. The exception exists for multicast audio sou will always be streaming audio. When an audio source is in use, even after the listener has disconnected will always have one input stream for each configured MOH codec. For u the stream may exist in a suspended state where no audio data is received connects to listen to the stream. Each MOH multicast resource uses one each audio source and codec combination. For example, if the default a configured for multicast, G.711 mu-law and wideband codecs, then two used (default audio source + G.711 mu-law and default audio source +
MOHConnectionsLost	This counter represents the total number of times since the last restart o Voice Media Streaming Application that a Unified Communications Ma connection was lost.
MOHConnectionState	For each Unified Communications Manager that is associated with an M counter represents the current registration state to Unified Communicati 0 indicates no registration to Unified Communications Manager; 1 indicat to the primary Unified Communications Manager; 2 indicates connecti secondary Unified Communications Manager (connected to Unified Co Manager but not registered until the primary Unified Communications connection fails).
MOHStreamsActive	This counter represents the total number of active (currently in use) sim direction) streams for all connections. One output stream exists for each listening to a unicast audio source, and one input stream exists for each source, multiplied by the number of MOH codecs. When an audio source has been used once, it will always have one inpu each configured MOH codec. For unicast streams, the stream may exist i state where no audio data is received until a device connects to listen to Each MOH multicast resource uses one stream for each audio source a combination. For example, if the default audio source is configured for G.711 mu-law and wideband codecs, then two streams get used (default + G.711 mu-law and default audio source + wideband).
MOHStreamsAvailable	This counter represents the remaining number of streams that are alloca MOH device that are available for use. This counter starts as 408 plus t configured half-duplex unicast connections and is reduced by 1 for each that started. The counter gets reduced by 2 for each multicast audio sour by the number of MOH codecs that are configured. The counter gets re each unicast audio source, multiplied by the number of MOH codecs co
MOHStreamsTotal	This counter represents the total number of simplex (one direction) stre connected to the MOH server since the Cisco IP Voice Media Streamin service started.

Counter	Counter Description
MTPConnectionsLost	This counter represents the total number of times since the last restart of th Voice Streaming Application that a Unified Communications Manager con was lost.
MTPConnectionState	For each Unified Communications Manager that is associated with an MTP, th represents the current registration state to Unified Communications Manager; no registration to Unified Communications Manager; 1 indicates registratio primary Unified Communications Manager; 2 indicates connection to the s Unified Communications Manager (connected to Unified Communications but not registered until the primary Unified Communications Manager con fails).
MTPConnectionsTotal	This counter represents the total number of MTP instances that have been sta the Cisco IP Voice Media Streaming Application service started.
MTPInstancesActive	This counter represents the number of active (currently in use) instances of
MTPStreamsActive	This counter represents the total number of currently active simplex (one d streams for all connections. Each stream direction counts as one stream.
MTPStreamsAvailable	This counter represents the remaining number of streams that are allocated MTP device that are available for use. This counter starts as 2 multiplied by th of configured connections (defined in the Cisco IP Voice Media Streaming A parameter for MTP, Call Count) and is reduced by one for each active strea
MTPStreamsTotal	This counter represents the total number of simplex (one direction) streams connected to the MTP device since the Cisco IP Voice Media Streaming Ap service started.
IVRInstancesActive	This represents the number of current active interactive voice responses.
IVRStreamsActive	This represents the total number of current active simplex (one direction) s all connections. Each stream direction counts as one stream. There is one in stream providing the audio input and another output stream to the endpoint
IVRStreamsAvailable	This represents the remaining number of streams allocated for the IVR devi available for use. This counter starts as 3 multiplied by the number of confi connections (defined in the Cisco IP Voice Media Streaming App service p for the IVR, Call Count) and is reduced by one for each active stream starte
IVRConnectionsTotal	This represents the total number of IVR instances that have been started since IP Voice Media Streaming Application service started.
IVRStreamsTotal	This represents the total number of simplex (one direction) streams that hav connected to the IVR device since the Cisco IP Voice Media Streaming Ap service started.
IVRConnectionsLost	This represents the total number of times the Unified Communications Ma connection was lost, since the last restart of the Cisco IP Voice Media Strea Application.

Counter	Counter Description
IVRErrors	This represents the total number of times the IVR failed to play, since t of the Cisco IP Voice Media Streaming Application.

Cisco Messaging Interface

The Cisco Messaging Interface object provides information about the Cisco Messaging Interface (CMI) service. The following table contains information on Cisco Messaging Interface (CMI) counters.

Table 41: Cisco Messaging Interface

Counters	Counter Description
HeartBeat	This counter represents the heartbeat of the CMI service. This incremer indicates that the CMI service is up and running. If the count does not i (increment), the CMI service is down.
SMDIMessageCountInbound	This counter represents the running count of inbound SMDI messages s restart of the CMI service.
SMDIMessageCountInbound24Hour	This counter represents the rolling count of inbound SMDI messages in hours.
SMDIMessageCountOutbound	This counter represents the running count of outbound SMDI messages restart of the CMI service.
SMDIMessageCountOutbound24Hour	This counter represents the rolling count of outbound SMDI messages i hours.
StartTime	This counter represents the time in milliseconds when the CMI service real-time clock in the computer, which simply acts as a reference point the current time and the time that has elapsed, in milliseconds, since the s provides the basis for this time. The reference point specifies midnight, 1970.

Cisco MGCP BRI Device

The Cisco Media Gateway Control Protocol (MGCP) Foreign Exchange Office (FXO) Device object provides information about registered Cisco MGCP BRI devices. The following table contains information on CiscoMGCP BRI device counters.

Table 42: Cisco MGCP BRI Device

Counters	Counter Description
CallsCompleted	This counter represents the total number of successful calls that were m MGCP Basic Rate Interface (BRI) device

Counters	Counter Description
Channel 1 Status	This counter represents the status of the indicated B-Channel that is associa the MGCP BRI device. Possible values: 0 (Unknown) indicates the status of t could not be determined; 1 (Out of service) indicates that this channel is no for use; 2 (Idle) indicates that this channel has no active call and is ready fo (Busy) indicates an active call on this channel; 4 (Reserved) indicates that th has been reserved for use as a D-channel or for use as a Synch-Channel for
Channel 2 Status	This counter represents the status of the indicated B-Channel that is associa the MGCP BRI device. Possible values: 0 (Unknown) indicates the status of t could not be determined; 1 (Out of service) indicates that this channel is no for use; 2 (Idle) indicates that this channel has no active call and is ready fo (Busy) indicates an active call on this channel; 4 (Reserved) indicates that th has been reserved for use as a D-channel or for use as a Synch-Channel for
DatalinkInService	This counter represents the state of the Data Link (D-Channel) on the corre digital access gateway. This value will get set to 1 (one) if the Data Link is service) or 0 (zero) if the Data Link is down (out of service).
OutboundBusyAttempts	This counter represents the total number of times that a call through this M device was attempted when no voice channels are available.

Cisco MGCP FXO Device

The Cisco Media Gateway Control Protocol (MGCP) Foreign Exchange Office (FXO) Device object provides information about registered Cisco MGCP FXO devices. The following table contains information on CiscoMGCP FXO device counters.

Table 43: Cisco MGCP FXO Device

Counters	Counter Description
CallsCompleted	This counter represents the total number of successful calls that were made port on an MGCP FXO device.
OutboundBusyAttempts	This counter represents the total number of times that a call through the por MGCP FXO device was attempted when no voice channels were available.
PortStatus	This counter represents the status of the FXO port associated with this MG device.

Cisco MGCP FXS Device

The Cisco MGCP Foreign Exchange Station (FXS) Device object provides information about registered Cisco MGCP FXS devices. One instance of this object gets created for each port on a Cisco Catalyst 6000 24 port FXS Analog Interface Module gateway. For example, a fully configured Catalyst 6000 Analog Interface Module would represent 24 separate instances of this object. The following table contains information on CiscoMGCP FXS device counters.

Table 44: Cisco MGCP FXS Device

Counters	Counter Description
CallsCompleted	This counter represents the total number of successful calls that were m port on the MGCP FXS device.
OutboundBusyAttempts	This counter represents the total number of times that a call through thi MGCP FXS device was attempted when no voice channels were availa
PortStatus	This counter represents the status of the FXS port that is associated with device.

Cisco MGCP Gateways

The Cisco MGCP Gateways object provides information about registered MGCP gateways. The following table contains information on CiscoMGCP gateway counters.

Table 45: Cisco MGCP Gateways

Counters	Counter Description
BRIChannelsActive	This counter represents the number of BRI voice channels that are curr a call in the gateway
BRISpansInService	This counter represents the number of BRI spans that are currently avai in the gateway.
FXOPortsActive	This counter represents the number of FXO ports that are currently acti the gateway.
FXOPortsInService	This counter represents the number of FXO ports that are currently avai in the gateway.
FXSPortsActive	This counter represents the number of FXS ports that are currently activ the gateway.
FXSPortsInService	This counter represents the number of FXS ports that are currently avai in the gateway.
PRIChannelsActive	This counter represents the number of PRI voice channels that are curr a call in the gateway.
PRISpansInService	This counter represents the number of PRI spans that are currently avai in the gateway.
T1ChannelsActive	This counter represents the number of T1 CAS voice channels that are cu in a call in the gateway.
T1SpansInService	This counter represents the number of T1 CAS spans that are currently use in the gateway.

Cisco MGCP PRI Device

The Cisco MGCP Primary Rate Interface (PRI) Device object provides information about registered Cisco MGCP PRI devices. The following table contains information on CiscoMGCP PRI device counters.

Table 46: Cisco MGCP PRI Device

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in use MGCP PRI device.
CallsCompleted	This counter represents the total number of successful calls that were made MGCP PRI device.
Channel 1 Status through Channel 15 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is associa MGCP PRI device. Possible values: 0 (Unknown) indicates that the status of t could not be determined; 1 (Out of service) indicates that this channel is not for use; 2 (Idle) indicates that this channel has no active call and is ready fo (Busy) indicates that an active call exists on this channel; 4 (Reserved) indi this channel has been reserved for use as a D-Channel or for use as a Synch for E-1.
Channel 16 Status	This counter represents the status of the indicated B-Channel that is associa MGCP PRI Device. Possible values: 0-Unknown, 1-Out of service, 2-Idle, 4-Reserved, for an E1 PRI Interface, this channel is reserved for use as a D
Channel 17 Status through Channel 31 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is associa the MGCP PRI Device. 0-Unknown, 1-Out of service, 2-Idle, 3-Busy, 4-Re
DatalinkInService	This counter represents the state of the Data Link (D-Channel) on the corre digital access gateway. This value will be set to 1 (one) if the Data Link is service) or 0 (zero) if the Data Link is down (out of service).
OutboundBusyAttempts	This counter represents the total number of times that a call through an MG device was attempted when no voice channels were available.

Cisco MGCP T1 CAS Device

The Cisco MGCP T1 Channel Associated Signaling (CAS) Device object provides information about registered Cisco MGCP T1 CAS devices. The following table contains information on CiscoMGCP TI CAS device counters.

Table 47: Cisco MGCP T1 CAS Device

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in use MGCP T1 CAS device.
CallsCompleted	This counter represents the total number of successful calls that were made MGCP T1 CAS device.

Counters	Counter Description
Channel 1 Status through Channel 24 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is ass an MGCP T1 CAS device. Possible values: 0 (Unknown) indicates the channel could not be determined; 1 (Out of service) indicates that this c available for use; 2 (Idle) indicates that this channel has no active call ar use; 3 (Busy) indicates that an active call exists on this channel; 4 (Reser that this channel has been reserved for use as a D-Channel or for use as a S for E-1.
OutboundBusyAttempts	This counter represents the total number of times that a call through the CAS device was attempted when no voice channels were available.

Cisco Mobility Manager

The Cisco Mobility Manager object provides information on registered Cisco Unified Mobility Manager devices. The following table contains information on Cisco Unified Mobility Manager device counters.

Table 48: Cisco Mobility Manager

Counters	Counter Description
MobileCallsAnchored	This counter represents the total number are associated with single-mode/dual-mo that is currently anchored on a Unified Co Manager. Call anchoring occurs when a enterprise gateway and connects to a mo application that then uses redirection to back out an enterprise gateway. For exa counter increments twice for a dual-mod phone-to-dual-mode phone call: once for t call and once for the terminating call. W terminates, this counter decrements acc
MobilityHandinsAborted	This counter represents the total number handins.
MobileHandinsCompleted	This counter represents the total number that were completed by dual-mode phones handin occurs when the call successfully the enterprise network and the phone mov to WLAN.
MobilityHandinsFailed	This counter represents the total number (calls on mobile devices that move from wireless network) that failed.
MobilityHandoutsAborted	This counter represents the total number handouts.

Counters	Counter Description
MobileHandoutsCompleted	This counter represents the total number of (calls on mobile devices that move from the WLAN network to the cellular network) tha completed. A completed handout occurs wh successfully connects.
MobileHandoutsFailed	This counter represents the total number of (calls on mobile devices that move from cell wireless network) that failed.
MobilityFollowMeCallsAttempted	This counter represents the total number of calls that were attempted.
MobilityFollowMeCallsIgnoredDueToAnswerTooSoon	This counter represents the total number of calls that were ignored before the AnswerTo timer went off.
MobilityIVRCallsAttempted	This counter represents the total number of IVR calls.
MobilityIVRCallsFailed	This counter represents the total number of calls.
MobilityIVRCallsSucceeded	This counter represents the total number of IVR calls.
MobilitySCCPDualModeRegistered	This counter represents the total number of SCCP devices that are registered.
MobilitySIPDualModeRegistered	This counter represents the total number of SIP devices that are registered.

Cisco Music On Hold (MOH) Device

The Cisco Music On Hold (MOH) Device object provides information about registered Cisco MOH devices. The following table contains information on CiscoMOH device counters.

Table 49: Cisco MOH Device

Counters	Counter Description
MOHHighestActiveResources	This counter represents the largest number of simultaneously active MOH co for an MOH server. This number includes both multicast and unicast conne
MOHMulticastResourceActive	This counter represents the number of currently active multicast connections to addresses that are served by an MOH server. Each MOH multicast resource uses one stream for each audio source and c combination. For example, if the default audio source is configured for mu G.711 mu-law and wideband codecs, two streams get used (default audio s G.711 mu-law and default audio source + wideband).

Counters	Counter Description
MOHMulticastResourceAvailable	This counter represents the number of multicast MOH connections to m addresses that are served by an MOH server that are not active and are s to be used now for the MOH server. Each MOH multicast resource uses one stream for each audio source ar combination. For example, if the default audio source is configured for G.711 mu-law and wideband codecs, two streams get used (default audi G.711 mu-law and default audio source + wideband).
MOHOutOfResources	This counter represents the total number of times that the Media Resour attempted to allocate an MOH resource when all available resources on servers that are registered with a Unified Communications Manager we active.
MOHTotalMulticastResources	This counter represents the total number of multicast MOH connections th to multicast addresses that are served by an MOH server. Each MOH multicast resource uses one stream for each audio source ar combination. For example, if the default audio source is configured for G.711 mu-law and wideband codecs, two streams get used (default audi G.711 mu-law and default audio source + wideband).
MOHTotalUnicastResources	This counter represents the total number of unicast MOH connections th by an MOH server. Each MOH unicast resource uses one stream.
MOHUnicastResourceActive	This counter represents the number of active unicast MOH connections server. Each MOH unicast resource uses one stream.
MOHUnicastResourceAvailable	This counter represents the number of unicast MOH connections that ar and are still available to be used now for an MOH server. Each MOH unicast resource uses one stream.

Cisco MTP Device

The Cisco Media Termination Point (MTP) Device object provides information about registered Cisco MTP devices. The following table contains information on CiscoMTP device counters.

Table 50: Cisco MTP Device

Counters	Counter Description
OutOfResources	This counter represents the total number of times that an attempt was ma an MTP resource from an MTP device and failed; for example, because were already in use.

Counters	Counter Description
ResourceActive	This counter represents the number of MTP resources that are currently in u for an MTP device. Each MTP resource uses two streams. An MTP in use represents one MTP that has been allocated for use in a call.
ResourceAvailable	This counter represents the total number of MTP resources that are not acti still available to be used now for an MTP device. Each MTP resource uses two streams. An MTP in use represents one MTP that has been allocated for use in a call.
ResourceTotal	This counter represents the total number of MTP resources that an MTP device This counter equals the sum of the counters ResourceAvailable and Resour

Cisco Phones

The Cisco Phones object provides information about the number of registered Cisco Unified IP Phones, including both hardware-based and other station devices.

The CallsAttempted counter represents the number of calls that have been attempted from this phone. This number increases each time that the phone goes off hook and on hook.

Cisco Presence Feature

The Cisco Presence object provides information about presence subscriptions, such as statistics that are related to the speed dial or call list Busy Lamp Field (BLF) subscriptions. The following table contains information on CiscoPresence feature.

Table 51: Cisco Presence

Counters	Counter Description
ActiveCallListAndTrunkSubscriptions	This counter represents the active presence subscriptions for the call list fe well as presence subscriptions through SIP trunk.
ActiveSubscriptions	This counter represents all active incoming and outgoing presence subscri
CallListAndTrunkSubscriptionsThrottled	This counter represents the cumulative number of rejected call list and trun presence subscriptions due to throttling for the call list feature.
IncomingLineSideSubscriptions	This counter represents the cumulative number of presence subscriptions t received on the line side.
IncomingTrunkSideSubscriptions	This counter represents the cumulative number of presence subscriptions t received on the trunk side.
OutgoingTrunkSideSubscriptions	This counter represents the cumulative number of presence subscriptions t sent on the trunk side.

Cisco QSIG Feature

The Cisco QSIG Feature object provides information about the operation of various QSIG features, such as call diversion and path replacement. The following table contains information about the Cisco QSIG feature counters.

Table 52: Cisco QSIG Feature

Counters	Counter Description
CallForwardByRerouteCompleted	This counter represents the number of successful calls that has been for rerouting. Call forward by rerouting enables the path for a forwarded ca optimized (minimizes the number of B-Channels in use) from the originato This counter resets when the CiscoCallManager service parameter Call Reroute Enabled is enabled or disabled, or when the Cisco CallManager Se
PathReplacementCompleted	This counter represents the number of successful path replacements that h Path replacement in a QSIG network optimizes the path between two ec (PBXs) that are involved in a call. This counter resets when the CiscoC service parameter Path Replacement Enabled is enabled or disabled, or w CallManager Service restarts.

Cisco Signaling Performance

The Cisco Signaling Performance object provides call-signaling data on transport communications on Unified Communications Manager. The following table contains information about the Cisco Signaling Performance counter.

Table 53: Cisco Signaling Performance

Counters	Counter Description
UDPPacketsThrottled	This counter represents the total number of incoming UDP packets that (dropped) because they exceeded the threshold for the number of incom per second that is allowed from a single IP address. Configure the thres SIP Station UDP Port Throttle Threshold and SIP Trunk UDP Port Throt service parameters in Cisco Unified Communications Manager Admini counter increments for every throttled UDP packet that was received si restart of the Cisco CallManager Service.

Cisco SIP

The Cisco Session Initiation Protocol (SIP) object provides information about configured SIP devices. The following table contains information on the CiscoSIP counters.

Table 54: Cisco SIP

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in use SIP device.
CallsAttempted	This counter represents the number of calls that have been attempted on this S including the successful and unsuccessful call attempts.
CallsCompleted	This counter represents the number of calls that were actually connected (a was established) from a SIP device. This number increments when the call is t
CallsInProgress	This counter represents the number of calls that are currently in progress o device, including all active calls. When all calls that are in progress are conn number of CallsInProgress equals the number of CallsActive.
VideoCallsActive	This counter represents the number of video calls with streaming video con that are currently active (in use) on this SIP device.
VideoCallsCompleted	This counter represents the number of video calls that were actually connec video streams for this SIP device. This number increments when the call is t

Cisco SIP Line Normalization

The Cisco SIP line normalization performance object contains counters that allow you to monitor aspects of the normalization script for SIP lines, including initialization errors, runtime errors, and script status. For SIP lines, each script has only one set of performance counters. This is true even if two endpoints share the same script. The following table contains information about the Cisco SIP line normalization counters.

Display Names	Description
DeviceResetAutomatically	This counter indicates the number of times that Unified Communications Manager automatically resets the device (SIP phone). Automatic resets occur only if the value specified in Script Execution Error Recovery Action or System Resource Error Recovery Action field is set to Reset Device. This counter increments each time Unified Communications Manager automatically resets a device (SIP phone) due to an error. The count is restarted when the script is reset following a change to the script configuration.

Display Names	Description
ErrorExecution	This counter indicates the number of execution errors that occur while the script executes. Execution errors can occur while a message handler executes. Execution errors can be caused by problems such as resource errors or an argument mismatch in a function call. When an execution error occurs, Unified Communications Manager performs the following actions: • Automatically restores the message to the original content before applying additional error-handling actions. • Increments the value of the counter. • Takes appropriate action based on the configuration of the Script Execution Error Recovery Action and System Resource Error Recovery Action fields in Cisco Unified Communications Manager Administration. Check the SIPNormalizationScriptError alarm for details, including the line number in the script that failed. Correct the script problem, upload the corrected script as needed, and reset the script by clicking the Reset button at the top of the script configuration page. The counter increments for each execution error since the last time the script was reset following a change to the script configuration. Both a script configuration change and a script reset must occur to restart the counter. If the counter continues to increment after you fix the script problem, examine the script again.
ErrorInit	This counter indicates the number of times a script error occurred after the script was successfully loaded into memory but failed to initialize in Unified Communications Manager. A script can fail to initialize due to resource errors, an argument mismatch in a function call, and so on. Check the SIPNormalizationScriptError alarm for details, including the line number in the script that failed. Correct the script problem, upload the corrected script if needed, and reset the script by clicking the Reset button at the top of the script configuration page. The counter for the script instance increments every time an initialization error occurs. This counter provides a count from the most recent script reset that was accompanied by a change to the script configuration. Both a script configuration change and a script reset must occur to restart the counter. If the counter continues to increment after you fix the script problem, examine the script again. When the error occurs during initialization, Unified Communications Manager automatically disables the script.
ErrorInternal	This counter indicates the number of internal errors that have occurred while the script executed. Internal errors are extremely rare. If the value in this counter is higher than zero, there is a defect in the system not related to the script content or execution. Collect SDI traces and contact the Technical Assistance Center (TAC).

Display Names	Description
ErrorLoad	This counter indicates the number of times that a script error occurred while the script loaded into memory in Unified Communications Manager. A script can fail to load due to memory issues or syntax errors; check the SIPNormalizationScriptError alarm for details such as the script line number where the syntax error exists, check the script for syntax errors, upload a corrected script if needed and reset the script by clicking the Reset button at the top of the script configuration page. The counter for the script instance increments for each load error since the last time the script was reset following a change to the script configuration. Both a script configuration change and a script reset must have occurred to restart the counter. If the counter continues to increment after you believe you have fixed the script problem, examine the script again.
ErrorResource	This counter indicates whether or not the script encountered a resource error. There are two kinds of resource errors: exceeding the value configured in the Memory Threshold field or exceeding the value configured in the Lua Instruction Threshold field. Both fields display in the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration. If either condition occurs, Unified Communications Manager immediately closes the script and issues the SIPNormalizationScriptError alarm. If a resource error occurs while the script loads or initializes, the script is disabled. If a resource error occurs during execution, the configured system resource error recovery action is taken as configured in the System Resource Error Recovery Action field on the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration.
MemoryUsage	This counter indicates the amount of memory, in bytes, that the script consumes based on the accumulation for all SIP phones using this script. This counter increases and decreases to match the amount of memory being utilized by the script. The count gets cleared when the script is closed (because a closed script consumes no memory) and restarts when the script is opened (enabled). A high number in this counter could indicate a resource problem. Check the MemoryUsagePercentage counter and check for a SIPNormalizationResourceWarning alarm, which occurs when the resource consumption exceeds an internally set threshold.

Display Names	Description
MemoryUsagePercentage	This counter indicates the percentage of the total amount of memory the script consumes based on the accumulation for all SIP phones using this script. The value in this counter is derived by dividing the value in the MemoryUsage counter by the value in the Memory Threshold field (in the SIP Normalization Script Configuration window) and multiplying that result by 100 to arrive at a percentage value. This counter increases and decreases in accordance with the MemoryUsage counter. This count is cleared when the script is closed (because closed scripts consume no memory) and restarts when the script is opened (enabled). When this counter reaches the internally controlled resource threshold, the SIPNormalizationResourceWarning alarm is issued.
MessageRollback	This counter indicates the number of times a message was not modified by the script due to an error while the script executes. This can occur only if the value in the Script Execution Error Recovery Action field is set to Message Rollback Only. When an execution error occurs, Unified Communications Manager automatically restores the message to the original contents prior to applying additional error-handling actions. If error handling specifies Rollback Only, no further action is taken beyond rolling back to the original message prior to the normalization attempt. For the other possible Script Execution Error Recovery Action settings, the action specified occurs after the message restores to the original contents.
msgAddContentBody	This counter indicates the number of times that the script adds a content body to the message. Assuming your message variable name is “msg”, if you are using the msg:addContentBody API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgAddHeader	This counter indicates the number of times that the script adds a SIP header to the message. Assuming your message variable name is “msg”, if you are using the msg:addHeader API in the script, this counter increases each time this API executes successfully. If the counter behavior is unexpected, examine the script logic for errors.
msgAddHeaderUriParameter	This counter indicates the number of times that the script adds a SIP header URI parameter to a SIP header in the message. Assuming your message variable name is “msg”, if you are using the msg:addHeaderUriParameter API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgAddHeaderValueParameter	This counter indicates the number of times that the script adds a SIP header value parameter to a SIP header in the message. Assuming your message variable name is “msg”, if you are using the msg:addHeaderValueParameter API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.

Display Names	Description
msgApplyNumberMask	This counter indicates the number of times that the script applies a number mask to a SIP header in the message. Assuming your message variable name is “msg”, if you are using the msg:applyNumberMask API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgBlock	This counter indicates the number of times that the script blocks a message. Assuming your message variable name is “msg”, if you are using the msg:block API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgConvertDiversiontoHl	This counter indicates the number of times that the script converts Diversion headers into History-Info headers in the message. Assuming your message variable name is “msg”, if you are using the msg:convertDiversionToHI API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgConvertHlToDiverion	This counter indicates the number of times that the script converts History-Info headers into Diversion headers in the message. Assuming your message variable name is “msg”, if you are using the msg:convertHIToDiversion API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgModifyHeader	This counter indicates the number of times that the script modifies a SIP header in the message. Assuming your message variable name is “msg”, if you are using the msg:modifyHeader API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgRemoveContentBody	This counter indicates the number of times that the script removes a content body from the message. Assuming your message variable name is “msg”, if you are using the msg:removeContentBody API in the script, this counter increases each time this API successfully executed. If the counter behavior is unexpected, examine the script logic for errors.
msgRemoveHeader	This counter indicates the number of times that the script removes a SIP header from the message. Assuming your message variable name is “msg”, if you are using the msg:removeHeader API in the script, this counter increases each time this API is successfully executed. If the counter behavior is unexpected, examine the script logic for errors.
msgRemoveHeaderValue	This counter indicates the number of times that the script removes a SIP header value from the message. Assuming your message variable name is “msg”, if you are using the msg:removeHeaderValue API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.

Display Names	Description
msgRemoveUnreliableSdp	This counter indicates the number of times that the script removes SDP body from an unreliable 18x SIP message. Assuming your message variable name is “msg”, if you are using the msg:removeUnreliableSDP API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgSetRequestUri	This counter indicates the number of times that the script modifies the request URI in the message. Assuming your message variable name is “msg”, if you are using the msg:setRequestUri API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgSetResponseCode	This counter indicates the number of times that the script modifies the response code or response phrase in the message. Assuming your message variable name is “msg”, if you are using the msg:setResponseCode API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgSetSdp	This counter indicates the number of times that the script sets the SDP in the message. Assuming your message variable name is “msg”, if you are using the msg:setSdp API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
ptAddContentBody	This counter indicates the number of times that the script adds a content body to the PassThrough object. Assuming your PassThrough object name is “pt”, if you are using the pt:addContentBody API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
ptAddHeader	This counter indicates the number of times that the script adds a SIP header to the PassThrough object. Assuming your PassThrough object name is “pt”, if you are using the pt:addHeader API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
ptAddHeaderUriParameter	This counter indicates the number of times that the script adds a SIP header URI parameter to the PassThrough object. Assuming your PassThrough object name is “pt”, if you are using the pt:addHeaderUriParameter API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
ptAddHeaderValueParameter	This counter indicates the number of times that the script adds a SIP header value parameter to the PassThrough object. Assuming your PassThrough object name is “pt”, if you are using the pt:addHeaderValueParameter API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.

Display Names	Description
ptAddRequestUriParameter	This counter indicates the number of times that the script adds a request URI parameter to the PassThrough object. Assuming your PassThrough object name is "pt", if you are using the pt:addRequestUriParameter API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
ScriptActive	This counter indicates whether the script is currently active (running on SIP phones). A value of 0 indicates that the script is closed (disabled). A value of 1 indicates that the script is open and operational. To open the script that should be running, check for any alarms that might indicate why the script is not open, correct any errors, upload a new script if necessary, and reset the script.
ScriptClosed	This counter indicates the number of times that Unified Communications Manager closes the script. When the script closes on one SIP phone, it can still be enabled on other SIP phones. Unified Communications Manager closes the script because the last SIP phone using this script was either reset manually, reset automatically (due to an error), or deleted. This count restarts when the script resets following a change to the script configuration and when Cisco CallManager restarts.
ScriptDisabledAutomatically	This counter indicates the number of times that the system automatically disables the script. The values that are specified in the Execution Error Recovery Action or System Resource Error Recovery Action field in the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration determine whether the script is disabled. Automatic script disable occurs if either of these fields are set to Disable Script. The script also gets disabled as a result of script error conditions that are encountered during loading and initialization. This counter provides a count from the most recent manual device reset that involves a script configuration change (a device reset alone does not restart the count; the script must also have changed before the reset occurs). The counter increments each time Unified Communications Manager automatically disables a script due because of script errors. If the number in this counter is higher than expected, perform the following steps: • Check for a SIPNormalizationScriptError alarm and SIPNormalizationAutoResetDisabled alarm. • Check for any resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files.

Display Names	Description
ScriptOpened	This counter indicates the number of times that Unified Communications Manager attempts to open the script. For the script to open, it must load into memory in Unified Communications Manager, initialize, and be operational. A number greater than 1 in this counter means that Unified Communications Manager has made more than one attempt to open this script either for an expected reason or due to an error during loading or initialization. The error can occur due to execution errors or resource errors or invalid syntax in the script. Expect this counter to be greater than 1 if the ScriptResetAutomatically counter increments. If the number in this counter is higher than expected, perform the following steps: • Check for alarms such as the SIPNormalizationScriptClosed, SIPNormalizationScriptError, or SIPNormalizationResourceWarning. • Check resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files. This count restarts when the script resets after a script configuration change and when Unified Communications Manager restarts.
ScriptResetAutomatically	This counter indicates the number of times that the system automatically resets the script. The script resets based on the values that are specified in the Script Execution Error Recovery Action and System Resource Error Recovery Action fields in the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration. Automatic resets can occur if the value in either of these fields is Reset Script. This counter specifies the number of times that the system automatically resets the script following the last time the script is reset after a change to the script configuration. The counter increments each time Unified Communications Manager automatically resets a script because of script errors. If the number in this counter is higher than expected, perform the following steps: • Check for a SIPNormalizationScriptError alarm. • Check for any resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files.
ScriptResetManually	This counter indicates the number of times that the script manually resets in Cisco Unified Communications Manager Administration or by other methods, such as AXL, or a reset on the last SIP phone that used the script. This counter increments when a script is reset due to configuration changes. This counter restarts when the script is deleted, or when Cisco CallManager restarts.

Cisco SIP Normalization

The Cisco SIP Normalization performance object contains counters that allow you to monitor aspects of the normalization script, including initialization errors, runtime errors, and script status. Each device that has an associated script causes a new instance of these counters to be created. The following table contains Unified Communications Manager the CiscoSIP Normalization counters.

Table 55: Cisco SIP Normalization

Display Name	Description
DeviceResetAutomatically	This counter indicates the number of times that Unified Communications Manage automatically resets the device (SIP trunk). The device reset is based on the value are specified in the Script Execution Error Recovery Action and System Resource Recovery Action fields on the SIP Normalization Script Configuration window in Unified Communications Manager Administration. When the device (SIP trunk) is due to script errors, the counter value increments. This count restarts when the dev reset manually.
DeviceResetManually	This counter indicates the number of times that the device (SIP trunk) is reset mar in Cisco Unified Communications Manager Administration or by other methods, as AXL. When the device associated with a script is reset due to configuration cha the counter value increments. The counter restarts in the following situations: • The SIP trunk is deleted. • The script on the trunk gets changed or deleted. • Unified Communications Manager restarts.
ErrorExecution	This counter represents the number of execution errors that occurred while the sc executed. Execution errors can occur while a message handler executes. Execution can be caused by resource errors, an argument mismatch in a function call, and sc When an execution error occurs, Unified Communications Manager performs the following actions: • Automatically restores the message to the original content before applying addi error handling actions. • Increments the value of the counter. • Takes appropriate action based on the configuration of the Script Execution Recovery Action and System Resource Error Recovery Action fields in Cisc Unified Communications Manager Administration. Check the SIPNormalizationScriptError alarm for details, including the line numb the script that failed. Correct the script problem, upload the corrected script as ne and reset the trunk. This counter increments every time an execution error occurs counter provides a count from the most recent trunk reset that involved a script configuration change. (A device reset alone does not restart the count; the script configuration must also change before the reset occurs.) If the counter continues to increment after you fix the script problem, examine the again.

Display Name	Description
ErrorInit	This counter represents the number of times a script error occurred after the sc successfully loaded into memory, but failed to initialize in Unified Communic Manager. A script can fail to initialize due to resource errors, an argument mis a function call, the expected table was not returned, and so on. Check the SIPNormalizationScriptError alarm for details, including the line n the script that failed. Correct the script problem, upload the corrected script as and reset the trunk. This counter increments every time an initialization error This counter provides a count from the most recent trunk reset that was accomp a script configuration change. (A device reset alone does not restart the count; configuration must also change before the reset occurs.) If the counter continu increment after you fix the script problem, examine the script again. When the occurs during initialization, Unified Communications Manager automatically the script.
ErrorInternal	This counter indicates the number of internal errors that occurred while the sc executed. Internal errors are very rare. If the value in this counter is higher tha defect exists in the system that is not related to the script content or execution SDI traces and contact the Technical Assistance Center (TAC).
ErrorLoad	This counter represents the number of times a script error occurred when the scri into memory in Unified Communications Manager. A script can fail to load d memory issues or syntax errors. Check the SIPNormalizationScriptError alarm for details. Check the script syn errors, upload the corrected script as needed, and reset the trunk. This counter in every time a load error occurs. This counter provides a count from the most rec reset that was accompanied by a script configuration change. (A device reset a not restart the count; the script configuration must also change before the rese If the counter continues to increment even after you fix the script problem, exa script again.
ErrorResource	This counter indicates whether the script encountered a resource error. Two kinds of resource errors exist: exceeding the value in the Memory Thresh and exceeding the value in the Lua Instruction Threshold field. (Both fields di the SIP Normalization Script Configuration window in Cisco Unified Commu Manager Administration.) If either condition occurs, Unified Communications immediately closes the script and issues the SIPNormalizationScriptError alar If a resource error occurs while the script loads or initializes, the script is disa resource error occurs during execution, the configured system resource error r action is taken. (The setting of the System Resource Error Recovery Action fie SIP Normalization Script Configuration window in Cisco Unified Communic Manager Administration defines this action.)

Display Name	Description
MemoryUsage	This counter specifies the amount of memory, in bytes, that the script consumes. counter increases and decreases to match the amount of memory that the script us This count gets cleared when the script closes (because a closed script does not cor memory) and restarts when the script opens (gets enabled). A high number in this co indicates a resource problem. Check the MemoryUsagePercentage counter and th SIPNormalizationResourceWarning alarm, which occur when the resource consum exceeds an internally set threshold.
MemoryUsagePercentage	This counter specifies the percentage of the total amount of memory that the scrip consumes. The value in this counter is derived by dividing the value in the MemoryUsage co by the value in the Memory Threshold field (in the SIP Normalization Script Configuration window) and multiplying the result by 100 to arrive at a percentag This counter increases and decreases in accordance with the MemoryUsage coun This count gets cleared when the script closes (because closed scripts do not cons memory) and restarts when the script opens (gets enabled). When this counter rea the internally controlled resource threshold, the SIPNormalizationResourceWarni alarm is issued.
MessageRollback	This counter indicates the number of times that the system automatically rolled ba message. The system rolls back the message by using the error handling that is spe in the Script Execution Error Recovery Action field in the SIP Normalization Scr Configuration window in Cisco Unified Communications Manager Administratio When an execution error occurs, Unified Communications Manager automatically re the message to the original content before applying additional error handling actio error handling specifies Rollback only, no further action is taken beyond rolling ba the original message before the normalization attempt. For the other possible Scri Execution Error Recovery Actions, message rollback always occurs first, followe the specified action, such as disabling the script, resetting the script automatically resetting the trunk automatically.
msgAddContentBody	This counter represents the number of times that the script added a content body t message. If you are using the msg:addContentBody API in the script, this counter increases each time that the msg:addContentBody API executes successfully. If th counter behavior is not as expected, examine the script logic for errors.
msgAddHeader	This counter represents the number of times that the script added a SIP header to message. If you are using the msg:addHeader API in the script, this counter incre each time that the msg:addHeader API executes successfully. If the counter behav not as expected, examine the script logic for errors.
msgAddHeaderUriParameter	This counter represents the number of times that the script added a SIP header UR parameter to a SIP header in the message. If you are using the msg:addHeaderUriParameter API in the script, this counter increases each time th msg:addHeaderUriParameter API executes successfully. If the counter behavior i as expected, examine the script logic for errors.

Display Name	Description
msgAddHeaderValueParameter	This counter represents the number of times that the script added a SIP header parameter to a SIP header in the message. If you are using the msg:addHeaderValueParameter API in the script, this counter increases each t the msg:addHeaderValueParameter API executes successfully. If the counter b is not as expected, examine the script logic for errors.
msgApplyNumberMask	This counter represents the number of times that the script applied a number m SIP header in the message. If you are using the msg:applyNumberMask API in t this counter increases each time that the msg:applyNumberMask API execute successfully. If the counter behavior is not as expected, examine the script log errors.
msgBlock	This counter represents the number of times that the script blocked a message are using the msg:block API in the script, this counter increases each time tha msg:block API executes successfully. If the counter behavior is not as expected the script logic for errors.
msgConvertDiversionToHI	This counter represents the number of times that the script converted Diversio into History-Info headers in the message. If you are using the msg:convertDiver API in the script, this counter increases each time that the msg:convertDiversi API executes successfully. If the counter behavior is not as expected, examine logic for errors.
msgConvertHIToDiversion	This counter represents the number of times that the script converted Diversio into History-Info headers in the message. If you are using the msg:convertDiver API in the script, this counter increases each time that the msg:convertDiversi API executes successfully. If the counter behavior is not as expected, examine logic for errors.
msgModifyHeader	This counter represents the number of times that the script modified a SIP hea message. If you are using the msg:modifyHeader API in the script, this counter each time that the msg:modifyHeader API executes successfully. If the counter is not as expected, examine the script logic for errors.
msgRemoveContentBody	This counter represents the number of times that the script removed a content b the message. If you are using the msg:removeContentBody API in the script, th increases each time that the msg:removeContentBody API executes successfu counter behavior is not as expected, examine the script logic for errors.
msgRemoveHeader	This counter represents the number of times that the script removed a SIP hea the message. If you are using the msg:removeHeader API in the script, this co increases each time that the msg:removeHeader API executes successfully. If th behavior is not as expected, examine the script logic for errors.
msgRemoveHeaderValue	This counter represents the number of times that the script removed a SIP hea from the message. If you are using the msg:removeHeaderValue API in the sc counter increases each time that the msg:removeHeaderValue API executes suc If the counter behavior is not as expected, examine the script logic for errors.

Display Name	Description
msgSetRequestUri	This counter represents the number of times that the script modified the request U the message. If you are using the msg:setRequestUri API in the script, this counte increases each time that the msg:setRequestUri API executes successfully. If the co behavior is not as expected, examine the script logic for errors.
msgSetResponseCode	This counter represents the number of times that the script modified the response and/or response phrase in the message. If you are using the msg:setResponseCod in the script, this counter increases each time that the msg:setResponseCode API exe successfully. If the counter behavior is not as expected, examine the script logic f errors.
msgSetSdp	This counter represents the number of times that the script set the SDP in the mes If you are using the msg:setSdp API in the script, this counter increases each time the msg:setSdp API executes successfully. If the counter behavior is not as expec examine the script logic for errors.
ptAddContentBody	This counter represents the number of times that the script added a content body t PassThrough (pt) object. If you are using the pt:addContentBody API in the scrip counter increases each time that the pt:addContentBody API executes successfull the counter behavior is not as expected, examine the script logic for errors.
ptAddHeader	This counter represents the number of times that the script added a SIP header to PassThrough (pt) object. If you are using the pt:addHeader API in the script, this co increases each time that the pt:addHeader API executes successfully. If the counte behavior is not as expected, examine the script logic for errors.
ptAddHeaderUriParameter	This counter represents the number of times that the script added a SIP header UI parameter to the PassThrough (pt) object. If you are using the pt:addHeaderUriPara API in the script, this counter increases each time that the pt:addHeaderUriParam API executes successfully. If the counter behavior is not as expected, examine the logic for errors.
ptAddHeaderValueParameter	This counter represents the number of times that the script added a SIP header va parameter to the PassThrough (pt) object. If you are using the pt:addHeaderValueParameter API in the script, this counter increases each time th pt:addHeaderValueParameter API executes successfully. If the counter behavior i as expected, examine the script logic for errors.
ptAddRequestUriParameter	This counter represents the number of times that the script added a request URI para to the PassThrough (pt) object. If you are using the pt:addRequestUriParameter A the script, this counter increases each time that the pt:addRequestUriParameter A executes successfully. If the counter behavior is not as expected, examine the script for errors.

Display Name	Description
ScriptActive	This counter indicates whether the script is currently active (running on the tr following values display for the counter: • 0—Indicates that the script is closed (disabled). • 1—Indicates that the script is open and operational. To open the script that should be running on this trunk, perform the following 1. Check for any alarms that might indicate why the script is not open. 2. Correct any errors. 3. Upload a new script if necessary. 4. Reset the trunk.
ScriptClosed	This counter indicates the number of times that Unified Communications Ma closed the script. When the script is closed, it is not enabled on this device. Unified Communications Manager closes the script under one of the following c • The device was reset manually. • The device was reset automatically (due to an error). • The device was deleted. This count restarts when the SIP trunk is reset after a change to the script con and when Unified Communications Manager restarts.
ScriptDisabledAutomatically	This counter indicates the number of times that the system automatically disa script. The values that are specified in the Script Execution Error Recovery A System Resource Error Recovery Action fields in the SIP Normalization Scri Configuration window in Cisco Unified Communications Manager Administ determine whether the script is disabled. The script also gets disabled as a resu error conditions that are encountered during loading and initialization. This c provides a count from the most recent manual device reset that involved a scr configuration change (a device reset alone does not restart the count; the script have changed before the reset occurs). This counter increments every time U Communications Manager automatically disables a script due to script errors. If the number in this counter is higher than expected, perform the following a • Check for SIPNormalizationScriptError alarm and SIPNormalizationAutoResetDisabled alarm. • Check for any resource-related alarms and counters in RTMT to determin a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace file

Display Name	Description
ScriptOpened	This counter indicates the number of times that the Unified Communications Ma attempted to open the script. For the a script to open, it must load into memory in U Communications Manager, initialize, and be operational. A number greater than this counter means that Unified Communications Manager has made more than o attempt to open the script on this SIP trunk, either for an expected reason or due t error during loading or initialization. The error can occur due to execution errors resource errors or invalid syntax in the script. Expect this counter to be greater tha if any of these counters increment: DeviceResetManually, DeviceResetAutomatic or ScriptResetAutomatically. The DeviceResetManually counter increments whe expected event, such as a maintenance window on the SIP trunk, causes the scrip close. If the number in this counter is high for an unexpected reason, perform the follow actions: • Check for alarms, such as the SIPNormalizationScriptClosed, SIPNormalizationScriptError, or SIPNormalizationResourceWarning. • Check resource-related alarms and counters in RTMT to determine whether resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files. This count restarts when the SIP trunk resets after a script configuration change a when Unified Communications Manager restarts.
ScriptResetAutomatically	This counter indicates the number of times that the system automatically reset the The script resets based on the values that are specified in the Script Execution Er Recovery Action and System Resource Error Recovery Action fields in the SIP Normalization Script Configuration window in Cisco Unified Communications Ma Administration. This counter specifies a count of the number of automatic script after the last manual device reset; this counter increments every time the Unified Communications Manager automatically resets a script due to script errors. If the number in this counter is higher than expected, perform the following actio • Check for a SIPNormalizationScriptError alarm. • Check for any resource-related alarms and counters in RTMT to determine wh a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files.

Cisco SIP Stack

The Cisco SIP Stack object provides information about Session Initiation Protocol (SIP) stack statistics that are generated or used by SIP devices such as SIP Proxy, SIP Redirect Server, SIP Registrar, and SIP User Agent. The following table contains information on Cisco SIP Stack counters.

Table 56: Cisco SIP Stack

Counters	Counter Description
AckIns	This counter represents the total number of ACK requests that the SIP device

Counters	Counter Description
AckOuts	This counter represents the total number of ACK requests that the SIP c
ByeIns	This counter represents the total number of BYE requests that the SIP de This number includes retransmission.
ByeOuts	This counter represents the total number of BYE requests that the SIP d This number includes retransmission.
CancelIns	This counter represents the total number of CANCEL requests that the received. This number includes retransmission.
CancelOuts	This counter represents the total number of CANCEL requests that the SI This number includes retransmission.
CCBsAllocated	This counter represents the number of Call Control Blocks (CCB) that a in use by the SIP stack. Each active SIP dialog uses one CCB.
GlobalFailedClassIns	This counter represents the total number of 6xx class SIP responses that t has received. This number includes retransmission. This class of respon that a SIP device, that is providing a client function, received a failure resp Generally, the responses indicate that a server had definitive information called party and not just the particular instance in the Request-URI.
GlobalFailedClassOuts	This counter represents the total number of 6xx class SIP responses that t sent. This number includes retransmission. This class of responses indic device, that is providing a server function, received a failure response m Generally, the responses indicate that a server had definitive information called party and not just the particular instance in the Request-URI.
InfoClassIns	This counter represents the total number of 1xx class SIP responses that t received. This includes retransmission. This class of responses provides on the progress of a SIP request.
InfoClassOuts	This counter represents the total number of 1xx class SIP responses that t sent. This includes retransmission. This class of responses provides info the progress of processing a SIP request.
InfoIns	This counter represents the total number of INFO requests that the SIP received. This number includes retransmission.
InfoOuts	This counter represents the total number of INFO requests that the SIP de This number includes retransmission.
InviteIns	This counter represents the total number of INVITE requests that the SI received. This number includes retransmission.
InviteOuts	This counter represents the total number of INVITE requests that the SI sent. This number includes retransmission.
NotifyIns	This counter represents the total number of NOTIFY requests that the S received. This number includes retransmission.

Counters	Counter Description
NotifyOuts	This counter represents the total number of NOTIFY requests that the SIP d sent. This number includes retransmission.
OptionsIns	This counter represents the total number of OPTIONS requests that the SIP received. This number includes retransmission.
OptionsOuts	This counter represents the total number of OPTIONS requests that the SIP d sent. This number includes retransmission.
PRAckIns	This counter represents the total number of PRACK requests that the SIP d received. This number includes retransmission.
PRAckOuts	This counter represents the total number of PRACK requests that the SIP d sent. This number includes retransmission.
PublishIns	This counter represents the total number of PUBLISH requests that the SIP received. This number includes retransmissions.
PublishOuts	This counter represents the total number of PUBLISH requests that the SIP d sent. This number includes retransmission
RedirClassIns	This counter represents the total number of 3xx class SIP responses that the S has received. This number includes retransmission. This class of responses information about redirections to addresses where the callee may be reacha
RedirClassOuts	This counter represents the total number of 3xx class SIP responses that the S has sent. This number includes retransmission. This class of responses prov information about redirections to addresses where the callee may be reacha
ReferIns	This counter represents the total number of REFER requests that the SIP de received. This number includes retransmission.
ReferOuts	This counter represents the total number of REFER requests that the SIP de sent. This number includes retransmission.
RegisterIns	This counter represents the total number of REGISTER requests that the SI has received. This number includes retransmission.
RegisterOuts	This counter represents the total number of REGISTER requests that the SI has sent. This number includes retransmission.
RequestsFailedClassIns	This counter represents the total number of 4xx class SIP responses that the S has received. This number includes retransmission. This class of responses a request failure by a SIP device that is providing a client function.
RequestsFailedClassOuts	This counter represents the total number of 4xx class SIP responses that the S has sent. This number includes retransmission. This class of responses indi request failure by a SIP device that is providing a server function.
RetryByes	This counter represents the total number of BYE retries that the SIP device To determine the number of first BYE attempts, subtract the value of this cou the value of the sipStatsByeOuts counter.

Counters	Counter Description
RetryCancels	This counter represents the total number of CANCEL retries that the SI sent. To determine the number of first CANCEL attempts, subtract the v counter from the value of the sipStatsCancelOuts counter.
RetryInfo	This counter represents the total number of INFO retries that the SIP de To determine the number of first INFO attempts, subtract the value of th from the value of the sipStatsInfoOuts counter.
RetryInvites	This counter represents the total number of INVITE retries that the SIP sent. To determine the number of first INVITE attempts, subtract the va counter from the value of the sipStatsInviteOuts counter.
RetryNotify	This counter represents the total number of NOTIFY retries that the SIP sent. To determine the number of first NOTIFY attempts, subtract the v counter from the value of the sipStatsNotifyOuts counter.
RetryPRAck	This counter represents the total number of PRACK retries that the SIP sent. To determine the number of first PRACK attempts, subtract the va counter from the value of the sipStatsPRAckOuts counter.
RetryPublish	This counter represents the total number of PUBLISH retries that the SI been sent. To determine the number of first PUBLISHs attempts, subtra of this counter from the value of the sipStatsPublishOuts counter.
RetryRefer	This counter represents the total number of REFER retries that the SIP de To determine the number of first REFER attempts, subtract the value of from the value of the sipStatsReferOuts counter.
RetryRegisters	This counter represents the total number of REGISTER retries that the S sent. To determine the number of first REGISTER attempts, subtract the counter from the value of the sipStatsRegisterOuts counter.
RetryRel1xx	This counter represents the total number of Reliable 1xx retries that the S sent.
RetryRequestsOut	This counter represents the total number of Request retries that the SIP de
RetryResponsesFinal	This counter represents the total number of Final Response retries that t has sent.
RetryResponsesNonFinal	This counter represents the total number of non-Final Response retries t device has sent.
RetrySubscribe	This counter represents the total number of SUBSCRIBE retries that the has sent. To determine the number of first SUBSCRIBE attempts, subtr of this counter from the value of the sipStatsSubscribeOuts counter.
RetryUpdate	This counter represents the total number of UPDATE retries that the SI sent. To determine the number of first UPDATE attempts, subtract the v counter from the value of the sipStatsUpdateOuts counter.

Counters	Counter Description
SCBsAllocated	This counter represents the number of Subscription Control Blocks (SCB) currently in use by the SIP stack. Each subscription uses one SCB.
ServerFailedClassIns	This counter represents the total number of 5xx class SIP responses that the has received. This number includes retransmission. This class of responses that failure responses were received by a SIP device that is providing a clien
ServerFailedClassOuts	This counter represents the total number of 5xx class SIP responses that the has sent. This number includes retransmission. This class of responses indi failure responses were received by a SIP device that is providing a server f
SIPGenericCounter1	Do not use this counter unless directed to do so by a Cisco Engineering Spe Cisco uses information in this counter for diagnostic purposes.
SIPGenericCounter2	Do not use this counter unless directed to do so by a Cisco Engineering Spe Cisco uses information in this counter for diagnostic purposes.
SIPGenericCounter3	Do not use this counter unless directed to do so by a Cisco Engineering Spe Cisco uses information in this counter for diagnostic purposes.
SIPGenericCounter4	Do not use this counter unless directed to do so by a Cisco Engineering Spe Cisco uses information in this counter for diagnostic purposes.
SIPHandlerSDLQueueSignalsPresent	This counter represents the number of SDL signals that are currently on the priority queues of the SIPHandler component. The SIPHandler component the SIP stack.
StatusCode1xxIns	This counter represents the total number of 1xx response messages, includi retransmission, that the SIP device has received. This count includes the fo 1xx responses: • 100 Trying • 180 Ringing • 181 Call is being forwarded • 182 Queued • 183 Session Progress
StatusCode1xxOuts	This counter represents the total number of 1xx response messages, includi retransmission, that the SIP device has sent. This count includes the follow responses: • 100 Trying • 180 Ringing • 181 Call is being forwarded • 182 Queued • 183 Session Progress

Counters	Counter Description
StatusCode2xxIns	This counter represents the total number of 2xx response messages, inc retransmission, that the SIP device has received. This count includes th 2xx responses: • 200 OK • 202 Success Accepted
StatusCode2xxOuts	This counter represents the total number of 2xx response messages, inc retransmission, that the SIP device has sent. This count includes the fol responses: • 200 OK • 202 Success Accepted
StatusCode3xxins	This counter represents the total number of 3xx response messages, inc retransmission, that the SIP device has received. This count includes th 3xx responses: • 300 Multiple Choices • 301 Moved Permanently • 302 Moved Temporarily • 303 Incompatible Bandwidth Units • 305 Use Proxy • 380 Alternative Service
StatusCode302Outs	This counter represents the total number of 302 Moved Temporarily respo including retransmission, that the SIP device has sent.

Counters	Counter Description
StatusCode4xxIns	This counter represents the total number of 4xx response messages, includi retransmission, that the SIP device has received. This count includes the fo 4xx responses: • 400 Bad Request • 401 Unauthorized • 402 Payment Required • 403 Forbidden • 404 Not Found • 405 Method Not Allowed • 406 Not Acceptable • 407 Proxy Authentication Required • 408 Request Timeout • 409 Conflict • 410 Gone • 413 Request Entity Too Large • 414 Request-URI Too Long • 415 Unsupported Media Type • 416 Unsupported URI Scheme • 417 Unknown Resource Priority • 420 Bad Extension • 422 Session Expires Value Too Small • 423 Interval Too Brief • 480 Temporarily Unavailable • 481 Call/Transaction Does Not Exist • 482 Loop Detected • 483 Too Many Hops • 484 Address Incomplete • 485 Ambiguous • 486 Busy Here • 487 Request Terminated • 488 Not Acceptable Here • 489 Bad Subscription Event • 491 Request Pending

Counters	Counter Description
StatusCode4xxOuts	This counter represents the total number of 4xx response messages, inc retransmission, that the SIP device has sent. This count includes the fol responses: • 400 Bad Request • 401 Unauthorized • 402 Payment Required • 403 Forbidden • 404 Not Found • 405 Method Not Allowed • 406 Not Acceptable • 407 Proxy Authentication Required • 408 Request Timeout • 409 Conflict • 410 Gone • 413 Request Entity Too Large • 414 Request-URI Too Long • 415 Unsupported Media Type • 416 Unsupported URI Scheme • 417 Unknown Resource Priority • 420 Bad Extension • 422 Session Expires Value Too Small • 423 Interval Too Brief • 480 Temporarily Unavailable • 481 Call/Transaction Does Not Exist • 482 Loop Detected • 483 Too Many Hops • 484 Address Incomplete • 485 Ambiguous • 486 Busy Here • 487 Request Terminated • 488 Not Acceptable Here • 489 Bad Subscription Event • 491 Request Pending
StatusCode5xxIns	This counter represents the total number of 5xx response messages, inc retransmission, that the SIP device has received. This count includes th 5xx responses: • 500 Server Internal Error • 501 Not Implemented • 502 Bad Gateway • 503 Service Unavailable • 504 Server Timeout • 505 Version Not Supported • 580 Precondition Failed

Counters	Counter Description
StatusCode5xxOuts	This counter represents the total number of 5xx response messages, includi retransmission, that the SIP device has sent. This count includes the follow responses: • 500 Server Internal Error • 501 Not Implemented • 502 Bad Gateway • 503 Service Unavailable • 504 Server Timeout • 505 Version Not Supported • 580 Precondition Failed
StatusCode6xxIns	This counter represents the total number of 6xx response messages, includi retransmission, that the SIP device has received. This count includes the fo 6xx responses: • 600 Busy Everywhere • 603 Decline • 604 Does Not Exist Anywhere • 606 Not Acceptable
StatusCode6xxOuts	This counter represents the total number of 6xx response messages, includi retransmission, that the SIP device has sent. This count includes the follow responses: • 600 Busy Everywhere • 603 Decline • 604 Does Not Exist Anywhere • 606 Not Acceptable
SubscribeIns	This counter represents the total number of SUBSCRIBE requests that the S has received. This number includes retransmission.
SubscribeOuts	This counter represents the total number of SUBSCRIBE requests that the S has sent. This number includes retransmission.
SuccessClassIns	This counter represents the total number of 2xx class SIP responses that the S has received. This includes retransmission. This class of responses provides in on the successful completion of a SIP request.
SuccessClassOuts	This counter represents the total number of 2xx class SIP responses that the S has sent. This includes retransmission. This class of responses provides inf on the successful completion of a SIP request.
SummaryRequestsIn	This counter represents the total number of SIP request messages that have received by the SIP device. This number includes retransmissions.

Counters	Counter Description
SummaryRequestsOut	This counter represents the total number of SIP request messages that th This number includes messages that originate on the device and messag being relayed by the device. When a particular message gets sent more th transmission gets counted separately; for example, a message that is re- retransmission or as a result of forking.
SummaryResponsesIn	This counter represents the total number of SIP response messages that t received. This number includes retransmission.
SummaryResponsesOut	This counter represents the total number of SIP response messages that t sent (originated and relayed). This number includes retransmission.
UpdateIns	This counter represents the total number of UPDATE requests that the S received. This number includes retransmission.
UpdateOuts	This counter represents the total number of UPDATE requests that the S sent. This number includes retransmission.

Cisco SIP Station

The Cisco SIP Station object provides information about SIP line-side devices. The following table contains information about the Cisco SIP Station counters.

Table 57: Cisco SIP Station

Counters	Counter Description
ConfigMismatchesPersistent	This counter represents the number of times that a phone that is running persistently unable to register due to a configuration version mismatch TFTP server and Unified Communications Manager since the last restart Communications Manager. This counter increments each time that Unif Communications Manager cannot resolve the mismatch and manual int required (such as a configuration update or device reset).
ConfigMismatchesTemporary	This counter represents the number of times that a phone that is running temporarily unable to register due to a configuration version mismatch TFTP server and Unified Communications Manager since the last restar CallManager Service. This counter increments each time Unified Comm Manager is able to resolve the mismatch automatically.
DBTimeouts	This counter represents the number of new registrations that failed beca occurred while the system was attempting to retrieve the device configu the database.
NewRegAccepted	This counter represents the total number of new REGISTRATION requ been removed from the NewRegistration queue and processed since the the Cisco CallManager Service.

Counters	Counter Description
NewRegQueueSize	This counter represents the number of REGISTRATION requests that are c on the NewRegistration queue. The system places REGISTRATION reques received from devices that are not currently registered on this queue before processed.
NewRegRejected	This counter represents the total number of new REGISTRATION requests rejected with a 486 Busy Here response and not placed on the NewRegistrat since the last restart of the Cisco CallManager Service. The system rejects REGISTRATION requests if the NewRegistration queue exceeds a program
TokensAccepted	This counter represents the total number of token requests that have been gra the last Unified Communications Manager restart. Unified Communications grants tokens as long as the number of outstanding tokens remains below th that is specified in the Cisco CallManager service parameter Maximum Phon Queue Depth.
TokensOutstanding	This counter represents the number of devices that have been granted a toke not yet registered. The system requires that devices that are reconnecting to priority Unified Communications Manager server be granted a token before re Tokens protect Unified Communications Manager from being overloaded w registration requests when it comes back online after a failover situation.
TokensRejected	This counter represents the total number of token requests that have been reje the last Unified Communications Manager restart. Unified Communications will reject token request if the number of outstanding tokens is greater than th that is specified in the Cisco CallManager service parameter Maximum Phon Queue Depth.

Cisco SW Conf Bridge Device

The Cisco SW Conference Bridge Device object provides information about registered Cisco software conference bridge devices. The following table contains information on the Cisco software conference bridge device counters.

Table 58: Cisco SW Conf Bridge Device

Counters	Counter Description
OutOfResources	This counter represents the total number of times that an attempt was made t a conference resource from a SW conference device and failed because all were already in use.
ResourceActive	This counter represents the number of resources that are currently in use (a a SW conference device. One resource represents one stream.
ResourceAvailable	This counter represents the total number of resources that are not active and available to be used now for a SW conference device. One resource represe stream.

Counters	Counter Description
ResourceTotal	This counter represents the total number of conference resources that a S device provides. One resource represents one stream.This counter equal the ResourceAvailable and ResourceActive counters.
SWConferenceActive	This counter represents the number of software-based conferences that active (in use) on a SW conference device.
SWConferenceCompleted	This counter represents the total number of conferences that have been released on a SW conference device. A conference starts when the first to the bridge. The conference completes when the last call disconnects fr

Cisco Telepresence MCU Conference Bridge Device

The Cisco Telepresence MCU Conference Bridge Device provides information about registered MCU conference bridge devices. The following table contains information about the Cisco Telepresence MCU Conference Bridge Device counters.

Table 59: Cisco Telepresence MCU Conference Bridge Device

Counters	Counter Description
ConferencesActive	This counter represents the total number of active conferences on all Cisco MCU conference bridge devices that are registered with Unified Comm Manager.
ConferencesCompleted	This counter represents the total number of conferences that used a Cisco MCU conference bridge allocated from Unified Communications Mana completed, implying that the conference bridge was allocated and released. is activated when the first call is connected to the bridge. The conference when the last call is disconnected from the bridge.
HttpConnectionErrors	This counter represents the total number of times Unified Communicati attempted to create HTTP connections to Cisco Telepresence MCU conf device, and failed due to connection errors on the Cisco Telepresence MC bridge side.
HttpNon200OKResponse	This counter represents the total number of times Unified Communicati received a non 200 OK HTTP Response from Cisco Telepresence MCU bridge, for any HTTP query sent.
OutOfResources	This counter represents the total number of times Unified Communicati attempted to allocate a conference resource from Cisco Telepresence MC bridge device and failed. For example, the attempt to allocate a confere fails, if all the resources are already in use.

Cisco TFTP Server

The Cisco Trivial File Transfer Protocol (TFTP) Server object provides information about the CiscoTFTP server. The following table contains information about Cisco TFTP server counters.

Table 60: Cisco TFTP Server

Counters	Counter Description
BuildAbortCount	This counter represents the number of times that the build process aborted v received a Build all request. This counter increases when building of device/unit/softkey/dial rules gets aborted as a result of group level change not
BuildCount	This counter represents the number of times since the TFTP service started TFTP server has built all the configuration files in response to a database c notification that affects all devices. This counter increases by one every time server performs a new build of all the configuration files.
BuildDeviceCount	This counter represents the number of devices that were processed in the la all the configuration files. This counter also updates while processing devic notifications. The counter increases when a new device is added and decrea an existing device is deleted. **Note** For 11.5 and above, you can built the configuration files and serv of caching. When a build happens, BuildDeviceCount increments. When t request from the phone, counter increases and never decreases stable monitoring is not required.
BuildDialruleCount	This counter represents the number of dial rules that were processed in the of the configuration files. This counter also updates while processing dial ru notifications. The counter increases when a new dial rule is added and decre an existing dial rule is deleted.
BuildDuration	This counter represents the time in seconds that it took to build the last con files.
BuildSignCount	This counter represents the number of security-enabled phone devices for v configuration file was digitally signed with the Unified Communications M server key in the last build of all the configuration files. This counter also u while processing security-enabled phone device change notifications.
BuildSoftKeyCount	This counter represents the number of softkeys that were processed in the l of the configuration files. This counter increments when a new softkey is a decrements when an existing softkey is deleted.
BuildUnitCount	This counter represents the number of gateways that were processed in the of all the configuration files. This counter also updates while processing un notifications. The counter increases when a new gateway is added and decre an existing gateway is deleted.
ChangeNotifications	This counter represents the total number of all the Unified Communications database change notifications that the TFTP server received. Each time tha configuration is updated in Unified Communications Manager, the TFTP s sent a database change notification to rebuild the XML file for the updated
DeviceChangeNotifications	This counter represents the number of times that the TFTP server received change notification to create, update, or delete configuration files for devic

Counters	Counter Description
DialruleChangeNotifications	This counter represents the number of times that the TFTP server receiv change notification to create, update, or delete configuration files for di
EncryptCount	This counter represents the number of configuration files that were encr counter gets updated each time a configuration file is successfully encry
GKFoundCount	This counter represents the number of GK files that were found in the c counter gets updated each time a GK file is found in the cache
GKNotFoundCount	This counter represents the number of GK files that were not found in th counter gets updated each time a request to get a GK file results in the cac it
HeartBeat	This counter represents the heartbeat of the TFTP server. This incremer indicates that the TFTP server is up and running. If the count does not i means that the TFTP server is down.
HttpConnectRequests	This counter represents the number of clients that are currently requesti GET file request.
HttpRequests	This counter represents the total number of file requests (such as reques configuration files, phone firmware files, audio files, and so on.) that the handled. This counter represents the sum total of the following counters HTTP service started: RequestsProcessed, RequestsNotFound, Request RequestsAborted, and RequestsInProgress.
HttpRequestsAborted	This counter represents the total number of HTTP requests that the HT canceled (aborted) unexpectedly. Requests could get aborted if the requ cannot be reached (for instance, the device lost power) or if the file tran interrupted due to network connectivity problems.
HttpRequestsNotFound	This counter represents the total number of HTTP requests where the re was not found. When the HTTP server does not find the requested file, a sent to the requesting device.
HttpRequestsOverflow	This counter represents the total number of HTTP requests that were re the maximum number of allowable client connections was reached. The have arrived while the TFTP server was building the configuration files some other resource limitation. The Cisco TFTP advanced service parame Serving Count, sets the maximum number of allowable connections.
HttpRequestsProcessed	This counter represents the total number of HTTP requests that the HT successfully processed.
HttpServedFromDisk	This counters represents the number of requests that the HTTP server co the files that are on disk and not cached in memory.
LDFoundCount	This counter represents the number of LD files that were found in the c counter gets updated each time a LD file is found in cache memory.

Counters	Counter Description
LDNotFoundCount	This counter represents the number of LD files that were not found in cache This counter gets updated each time a request to get an LD file results in the finding it.
MaxServingCount	This counter represents the maximum number of client connections that the serve simultaneously. The Cisco TFTP advanced service parameter, Maximu Count, sets this value.
Requests	This counter represents the total number of file requests (such as requests f configuration files, phone firmware files, audio files, and so on.) that the TF handles. This counter represents the sum total of the following counters since service started: RequestsProcessed, RequestsNotFound, RequestsOverflow RequestsAborted, and RequestsInProgress.
RequestsAborted	This counter represents the total number of TFTP requests that the TFTP serve (aborted) unexpectedly. Requests could be aborted if the requesting device reached (for instance, the device lost power) or if the file transfer was interr to network connectivity problems.
RequestsInProgress	This counter represents the number of file requests that the TFTP server cu processing. This counter increases for each new file request and decreases file request that is completed. This counter indicates the current load of the server.
RequestsNotFound	This counter represents the total number of TFTP requests for which the req was not found. When the TFTP server does not find the requested file, a me sent to the requesting device. If this counter increments in a cluster that is c as secure, this event usually indicates an error condition. If, however, the cl configured as non-secure, it is normal for the CTL file to be absent (not foun results in a message being sent to the requesting device and a corresponding in this counter. For non-secure clusters, then, this normal occurrence does no an error condition.
RequestsOverflow	This counter represents the total number of TFTP requests that were rejecte the maximum number of allowable client connections was exceeded, becaus arrived while the TFTP server was building the configuration files, or becaus other resource limitation. The Cisco TFTP advanced service parameter, Ma Serving Count, sets the maximum number of allowable connections.
RequestsProcessed	This counter represents the total number of TFTP requests that the TFTP se successfully processed.
SegmentsAcknowledged	This counter represents the total number of data segments that the client de acknowledged. Files get sent to the requesting device in data segments of 5 and for each 512-byte segment, the device sends the TFTP server an acknow message. Each additional data segment gets sent upon receipt of the acknow for the previous data segment until the complete file successfully gets trans the requesting device.
SegmentsFromDisk	This counter represents the number of data segments that the TFTP server r the files on disk, while serving files.

Counters	Counter Description
SegmentSent	This counter represents the total number of data segments that the TFTI Files get sent to the requesting device in data segments of 512 bytes.
SEPFoundCount	This counter represents the number of SEP files that were successfully cache. This counter gets updated each time that a SEP file is found in th
SEPNotFoundCount	This counter represents the number of SEP files that were not found in th counter gets updated each time that a request to get a SEP file produces in cache memory result.
SIPFoundCount	This counter represents the number of SIP files that were successfully f cache. This counter gets updated each time that a SIP file is found in th
SIPNotFoundCount	This counter represents the number of SIP files that were not found in th counter gets updated each time that a request to get a SIP file produces cache memory result.
SoftkeyChangeNotifications	This counter represents the number of times that the TFTP server receiv change notification to create, update, or delete configuration files for so
UnitChangeNotifications	This counter represents the number of times that the TFTP server receiv change notification to create, update, or delete gateway-related configu

Cisco Transcode Device

The Cisco Transcode Device object provides information about registered Cisco transcoding devices. The following table contains information on Cisco transcoder device counters.

Table 61: Cisco Transcode Device

Counters	Counter Description
OutOfResources	This counter represents the total number of times that an attempt was ma a transcoder resource from a transcoder device and failed; for example, resources were already in use.
ResourceActive	This counter represents the number of transcoder resources that are curr (active) for a transcoder device. Each transcoder resource uses two streams.
ResourceAvailable	This counter represents the total number of resources that are not active available to be used now for a transcoder device. Each transcoder resource uses two streams.
ResourceTotal	This counter represents the total number of transcoder resources that a t device provided. This counter equals the sum of the counters ResourceA ResourceAvailable.

Cisco Video Conference Bridge

The Cisco Video Conference Bridge object provides information about registered Cisco video conference bridge devices. The following table contains information on Cisco video conference bridge device counters.

Table 62: Cisco Video Conference Bridge

Counters	Counter Description
ConferencesActive	This counter represents the total number of video conferences that are curre (in use) on a video conference bridge device. The system specifies a confe active when the first call connects to the bridge.
ConferencesAvailable	This counter represents the number of video conferences that are not active still available on a video conference device.
ConferencesCompleted	This counter represents the total number of video conferences that have beer and released on a video conference device. A conference starts when the fi connects to the bridge. The conference completes when the last call disconn the bridge.
ConferencesTotal	This counter represents the total number of video conferences that are conf a video conference device.
OutOfConferences	This counter represents the total number of times that an attempt was made a video conference from a video conference device and failed because the already had the maximum number of active conferences that is allowed (as by the TotalConferences counter).
OutOfResources	This counter represents the total number of times that an attempt was made a conference resource from a video conference device and failed, for exampl all resources were already in use.
ResourceActive	This counter represents the total number of resources that are currently acti on a video conference bridge device. One resource gets used per participan
ResourceAvailable	This counter represents the total number of resources that are not active an available on a device to handle additional participants for a video conferen device.
ResourceTotal	This counter represents the total number of resources that are configured o conference bridge device. One resource gets used per participant.

Cisco Web Dialer

The Cisco WebDialer object provides information about the Cisco Web Dialer application and the Redirector servlet. The following table contains information on the CiscoWebDialer counters.

Table 63: Cisco Web Dialer

Counters	Counter Description
CallsCompleted	This counter represents the number of Make Call and End Call requests Web Dialer application successfully completed.
CallsFailed	This counter represents the number of Make Call and End Call requests unsuccessful.
RedirectorSessionsHandled	This counter represents the total number of HTTP sessions that the Red handled since the last service startup.
RedirectorSessionsInProgress	This counter represents the number of HTTP sessions that are currently b by the Redirector servlet.
RequestsCompleted	This counter represents the number of Make Call and End Call requests WebDialer servlet has successfully completed.
RequestsFailed	This counter represents the number of Make Call and End Call requests
SessionsHandled	This counter represents the total number of CTI sessions that the Cisco servlet handled since the last service startup.
SessionsInProgress	This counter represents the number of CTI sessions that the Cisco Web is currently servicing.

Cisco WSM Connector

The WSM object provides information on WSMConnectors that are configured on Unified Communications Manager. Each WSMConnector represents a physical Motorola WSM device. The following table contains information on the CiscoWSM Connector counters.

Table 64: Cisco WSM Connector

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in WSMConnector device.
CallsAttempted	This counter represents the number of calls that have been attempted or WSMConnector device, including both successful and unsuccessful cal
CallsCompleted	This counter represents the number of calls that are connected (a voice established) through the WSMConnector device. The counter incremen call terminates.
CallsInProgress	This counter represents the number of calls that are currently in progres WSMConnector device. This includes all active calls. When the numbe CallsInProgress equals the number of CallsActive, this indicates that al connected.

Counters	Counter Description
DMMSRegistered	This counter represents the number of DMMS subscribers that are registere WSM.

IME Client

The IME Client object provides information about the Cisco IME client on the Unified Communications Manager server. The following table contains information on the Cisco IME client counters.

Table 65: Cisco IME Client

Counters	Counter Description
CallsAccepted	This counter indicates the number of Cisco IME calls that the Unified Comm Manager received successfully and that the called party answered, resulting call.
CallsAttempted	This counter indicates the number of calls that the Unified Communications received through Cisco IME. This number includes accepted calls, failed ca busy, no-answer calls. The counter increments each time that Unified Comm Manager receives a call through Cisco IME.
CallsReceived	This counter indicates the number of calls that Unified Communications M receives through Cisco IME. This number includes accepted calls, failed ca busy, no-answer calls. The counter increments on call initiation.
CallsSetup	This counter indicates the number of Cisco IME calls that Unified Commu Manager placed successfully and that the remote party answered, resulting call.
DomainsUnique	This counter indicates the number of unique domain names of peer enterpris Cisco IME client discovered. The counter serves as an indicator of overall usage.
FallbackCallsFailed	This counter indicates the total number of failed fallback attempts.
FallbackCallsSuccessful	This counter indicates the total number of Cisco IME calls that have fallen b PSTN mid-call due to a quality problem. The counter includes calls initiated received by this Unified Communications Manager.
IMESetupsFailed	This counter indicates the total number of call attempts for which a Cisco I was available but that were set up through the PSTN due to a failure to con target over the IP network.
RoutesLearned	This counter indicates the total number of distinct phone numbers that the C has learned and that are present as routes in the Unified Communications M routing tables. If this number grows too large, the server may exceed the pe limit, and you may need to add additional servers to your cluster.

Counters	Counter Description
RoutesPublished	This counter indicates the total number of DIDs that were published suc the IME distributed cache across all Cisco IME client instances. The cou a dynamic measurement that gives you an indication of your own provi and a sense of how successful the system has been in storing the DIDs ir
RoutesRejected	This counter indicates the number of learned routes that were rejected b administrator restricted the particular number or domain. This counter p indication of the number of cases where a VoIP call cannot happen in the f of the blocked validation.
VCRUploadRequests	This counter indicates the number of voice call record (VCR) upload rec Unified Communications Manager has sent to the Cisco IME server to the IME distributed cache.

IME Client Instance

The IME Client Instance object provides information about the Cisco IME client instance on the Unified Communications Manager server. The following table contains information on the Cisco IME client instance counters.

Table 66: IME Client

Counters	Counter Description
IMEServiceStatus	This counter indicates the overall health of the connection to the Cisco for a particular Cisco IME client instance (Unified Communications Ma following values may display for the counter: • 0—Indicates an unknown state (which may mean that the Cisco IM not active). If the value specifies 0, an alert gets generated once per hour while t remains in the unknown state. • 1—Indicates a healthy state; that is, the Cisco IME service is activ Unified Communications Manager has successfully established a c its primary and backup servers for the Cisco IME client instance, i • 2—Indicates an unhealthy state; that is, the Cisco IME service is a Unified Communications Manager has not successfully established to its primary and backup servers for the Cisco IME client instance,

SAML Single Sign-On

The following table contains information about SAML Single Sign-On counters.

Table 67: SAML Single Sign-On Counters

Counter	Counter description
SAML_REQUESTS	This counter represents the total number of SAML requests sent to the configured Identity Provider.
SAML_RESPONSES	This counter represents the total number of SAML responses received from the configured Identity Provider.

Additionally, the following SAML SSO counters are also displayed in the Unified RTMT but they are not functional in Unified Communications Manager 10.0(1):

- OAUTH_TOKENS_ISSUED
- OAUTH_TOKENS_ACTIVE
- OAUTH_TOKENS_VALIDATED
- OAUTH_TOKENS_EXPIRED
- OAUTH_TOKENS_REVOKED

Cisco IVR Device

This object provides information about registered Cisco Interactive Voice Response (IVR) devices.

Counters	Counter Description
ResourceTotal	This represents the total number of IVR resources configured for this IVR device.
ResourceActive	This represents the total number of IVR resources that are currently active for this IVR device.
ResourceAvailable	This represents the total number of resources that are not active and are still available to be used at the current time for the IVR device.
OutOfResources	This represents the total number of times an attempt was made to allocate an IVR resource from this IVR device and failed, because all the resources were in use.

IM and Presence Service Counters

Cisco Client Profile Agent

This object provides information about the Cisco Client Profile (SOAP) interface.

The following table contains information about client profile agent counters.

Table 68: Cisco Client Profile Agent counters

Counters	Counter Descriptions
SoapCrossClusterRedirect	This counter represents the number of login requests recei in a peer cluster.
SoapLoginFailures	This counter represents the number of failed login reques
SoapNodeRedirect	This counter represents the number of login requests receiv node.

Cisco Presence Engine

The Cisco Presence Engine object provides information about the SIP messages that the Presence Engine receives and sends.

The following table contains information about Cisco Presence Engine performance counters.

Table 69: Cisco Presence Engine counters

Counters	Counter Description
Subscribe	
SubscribesReceived	This counter represents the number of SUBSCRIBE messages re refreshes, fetches & unsubscribes.
SubscribesSent	This counter represents the total number of SUBSCRIBE mess
SubscribesReceivedPresence	This counter represents the number of SUBSCRIBE messages presence.
SubscribesReceivedProfileConfig	This counter represents the number of SUBSCRIBE messages profileconfig.
SubscribesInitial	This counter represents the number of initial non-calendar SU
SubscribesRefresh	This counter represents the number of non-calendar refresh SU
SubscribesFetch	This counter represents the number of non-calendar fetch SUB
SubscribesRemove	This counter represents the number of non-calendar remove SU

Counters	Counter Description
ActiveSubscriptions	This counter represents the number of non-calendar subscriptions
SubscribesRedirect3xx	This counter represents the number of SUBSCRIBE messages red
SubscribesRejected4xx	This counter represents the number of SUBSCRIBE messages rej
SubscibesRejected5xx	This counter represents the number of SUBSCRIBE messages rej
SubscibesRejected6xx	This counter represents the number of SUBSCRIBE messages rej
SubcribesRejectedWith503	This counter represents the number of SUBSCRIBE messages rej
SubscriptionActiveSentForeign	This counter represents the number of active subscriptions sent by
SubscriptionActiveReceivedFrom Foreign	This counter represents the number of active subscriptions receive
WatcherInfoPresenceSubscriptions	This counter represents the number of watcher-info presence subs
Calendar	
ActiveCalendarSubscriptions	This counter represents the n.umber of calendar subscriptions that
SubscribesSentCalendarInitial	This counter represents the number of initial SUBSCRIBE messag
SubscribesSentCalendarRefresh	This counter represents the number of refresh SUBSCRIBE messa
SubscribesSentCalendarRetry	This counter represents the number of retry SUBSCRIBE message
SubscribesReceivedCalendar	This counter represents the number of SUBSCRIBE messages rec calendar.
NotifiesReceivedCalendar	This counter represents the number of NOTIFY messages by the
NotifiesSentCalendar	This counter represents the number of NOTIFY messages sent fro
MeetingsStarted	This counter represents the number of meetings that were started t
MeetingsEnded	This counter represents the number of meetings that were ended th
Publish	
PublicationsProcessed	This counter represents the number of successful publications pro
PublishInitial	This counter represents the number of initial PUBLISH messages
PublishRefresh	This counter represents the number of refresh PUBLISH message
PublishModify	This counter represents the number of modify PUBLISH message
PublishRemove	This counter represents the number of remove PUBLISH message
Notify	
NotificationsInQueue	This counter represents the number of the existing number of outgo

Counters	Counter Description
NotifiesSent	This counter represents the number of successful NOTIFY me
NotifiesReceived	This counter represents the number of NOTIFY messages rece
NotifiesSentPresence	This counter represents the number of NOTIFY messages sent
NotifiesSentProfileConfig	This counter represents the number of NOTIFY messages sent fr
NotifiesRetried	This counter represents the number of NOTIFY messages sent
NotifiesTimedouts	This counter represents the number of NOTIFY messages that
NotifiesRejected3xx	This counter represents the number of NOTIFY messages reje
NotifiesRejected4xx	This counter represents the number of NOTIFY messages reje
NotiffiesRejected5xx	This counter represents the number of NOTIFY messages reje
NotifiesRejected503	This counter represents the number of NOTIFY messages reje
NotifiesRejected6xx	This counter represents the number of NOTIFY messages reje
WatcherInfoPresenceNotifications	This counter represents the number of watcher-info presence n
WatcherInfoPresenceSubscriptions	This counter represents the number of watcher-info presence s
HighWaterMark	
HighWaterMark	This counter represents the number of times the load high wat
Active Views	
ActiveViews	This counter represents the number of Active Views in the Pre
Active Resources	
ActiveResources	This counter represents the number of active resources in the F
JSM	
ActiveJsmSessions	This counter represents the number of client emulation session
XMPP	
XMPPPresenceReceived	This counter represents the number of XMPP presence packets
XMPPPresenceFiltered	This counter represents the number of XMPP presence packets
XMPPPresenceNotificationsSent	This counter represents the number of composed presence upd
XMPPIMReceived	This counter represents the number of XMPP Instant Message
XMPPIMSent	This counter represents the number of XMPP Instant Message
XMPPIMTcInviteErrors	This counter represents the number of XMPP TC Invites rejec

Counters	Counter Description
XMPPIMResourceNotFoundErrors	This counter represents the number of XMPP Instant Message pac
XMPPIMIgnored	This counter represents the number of XMPP Instant Message pac
XMPPIMGoneGenerated	This counter represents the number of gone messages sent to the F
RFIErrors	This counter represents the number of errors when sending XMPP
RFIMessageQueueSize	This counter represents the current number of XMPP Messages th
SIP	
SIPIMReceived	This counter represents the number of SIP Instant Message packet
SIPIMSent	This counter represents the number of SIP Instant Message packet
SIPIMGoneGenerated	This counter represents the number of gone messages sent to the F
SIPIMRetry	This counter represents the number of SIP Instant Message resent
SIPIMTimeout	This counter represents the number of SIP Instant Message packet
SIPIMReject3xx	This counter represents the number of 3xx errors when attempting
SIPIMReject4xx	This counter represents the number of 4xx errors when attempting
SIPIMReject5xx	This counter represents the number of 5xx errors when attempting
SIPIMReject6xx	This counter represents the number of 6xx errors when attempting
ActiveIMSessions	This counter represents the number of Active Instant Message ses
Roster Sync	
RosterSyncAddBuddySuccess	This counter represents the number of successful add buddy reque
RosterSyncAddBuddyFailure	This counter represents the number of failed add buddy requests p
RosterSyncUpdateBuddySuccess	This counter represents the number of successful update buddy re
RosterSyncUpdateBuddyFailure	This counter represents the number of failed update buddy request
RosterSyncDeleteBuddySuccess	This counter represents the number of successful delete buddy req
RosterSyncDeleteBuddyFailure	This counter represents the number of failed delete buddy requests
RosterSyncSubscribeSuccess	This counter represents the number of successful subscribe reques
RosterSyncSubscribeFailure	This counter represents the number of failed subscribe requests pr
RosterSyncUnSubscribeSuccess	This counter represents the number of successful unsubscribe requ
RosterSyncUnSubscribeFailure	This counter represents the number of failed unsubscribe requests
PolicyUpdateSent	This counter represents the number of privacy policy update sent t

Counters	Counter Description
PolicyUpdateReceived	This counter represents the number of privacy policy update re
RosterSyncUnSubscribedSuccess	This counter represents the number of successful unsubscribed
RosterSyncUnSubscribedFailure	This counter represents the number of failed unsubscribed requ

Cisco Server Recovery Manager

This object provides information about the Cisco Server Recovery Manager (SRM) state. The following table contains information about SRM counters.

Table 70: Cisco Server Recovery Manager Counters

Counters	Counter Descriptions
SRMState	This counter represents the state of the SRM. • 0 = Unknown • 1 = Initializing • 2 = Idle • 3 = Active Normal • 4 = Backup Activated • 5 = Taking Over • 6 = Taking Back • 7 = Failing Over • 8 = Failed Over • 9 = Failed Over Affected Service • 10 = Falling Back • 11 = Failed • 12 = Down State

Cisco SIP Proxy

The following table contains information about Cisco SIP Proxy counters.

Table 71: Proxy counters

Counters	Counter Descriptions
CTIGWConferenceReq	This counter represents the number of conference call reques

Counters	Counter Descriptions
CTIGWInboundCalls	This counter represents the number of inbound calls received by
CTIGWLineOpenRequest	This counter represents the number of LineOpen requests receive
CTIGWMakeCallRequest	This counter represents the number of MakeCall requests receive
CTIGWRefreshCount	This counter represents the number of INVITE Refreshes receive MOC client.
CTIGWRetrieveReq	This counter represents the number of retrieve call requests recei
CTIGWSip4XXRes	This counter represents the number of SIP 4XX response sent by
CTIGWSip5XXRes	This counter represents the number of SIP 5XX response sent by
CTIGWSSXrefReq	This counter represents the number of single step transfer call re
CTIGWUsersAuthorized	This counter represents the number of users authorized by CTIG
CTIGWUsersCurrentlyAuthorized	This counter represents the number of users currently logged into
CTIGWXrefReq	This counter represents the number of transfer call requests recei
HttpRequests	This counter represents the number of HTTP requests processed.
IMCTRLActiveSessions	This counter represents the current number of active federated IM
IMGWActiveSessions	This counter represents the current number of active SIP XMPP
IMGWClientMessageSent	This counter represents the current number of SIP Messages sent
IMGWPeMessageReceived	This counter represents the current number of SIP Messages rece
IMGWPeMessageSent	This counter represents the current number of SIP Messages sent
Ipc_Requests	This counter represents the number of IPC requests from the TCI
NumIdleSipdWorkers	This counter represents the number of idle sipd worker processes
NumSipdWorker	This counter represents the number of sipd worker processes at a
Proxy_Due_Timer_Events	This counter represents the number of past-due timer events that
Proxy_Timer_Events	This counter represents the number of expired timer events.
PWSAppUserLoginRequest	This counter represents the number of Application User login rec
PWSAppUserLogoutRequest	This counter represents the number of Application User logout re
PWSEndpointExpired	This counter represents the number of subscriptions that expire b
PWSEndpointRefreshRequest	This counter represents the number of Endpoint refresh requests
PWSEndUserLoginRequest	This counter represents the number of End User login requests re

Counters	Counter Descriptions
PWSEndUserLogoutRequest	This counter represents the number of End User logout reque
PWSGetPolledPresenceRequest	This counter represents the number of GetPolledPresence req
PWSGetSubscribedPresenceRequest	This counter represents the number of GetSubscribedPresenc
PWSPresenceNotifies	This counter represents the number of Presence Notifications
PWSRegisterEndpointRequest	This counter represents the number of Register Endpoint requ
PWSSetPresenceRequest	This counter represents the number of SetPresence requests r
PWSSipNotifies	This counter represents the number of SIP Notifies received l
PWSSipPublishRequests	This counter represents the number of SIP Publish requests s
PWSSipSubscribeRequests	This counter represents the number of SIP Subscribe requests
PWSSipUnpublishRequests	This counter represents the number of SIP Unpublish request
PWSSipUnsubscribeRequests	This counter represents the number of SIP Unsubscribe reque
PWSSubscribeExpired	This counter represents the number of endpoint registrations
PWSSubscribeRefreshRequest	This counter represents the number of Subscribe refresh requ
PWSSubscribeRequest	This counter represents the number of Subscribe requests rec
PWSUnregisterEndpointRequest	This counter represents the number of Unregister Endpoint re
PWSUnsubscribeRequest	This counter represents the number of Unsubscribe requests r
ServerLoadStatus	This counter represents the Server load status on scale of 0 (i
SIPClientImMessage	This counter represents the number of SIP Client Instant Mes
SIPClientRegistered	This counter represents the number of SIP Client REGISTER
SIPClientRegisterFailed	This counter represents the number of failed SIP Client REG
Sip_Tcp_Requests	This counter represents the number of sip requests received o
Sip_Udp_Requests	This counter represents the number of sip requests received o
SIPInviteRequestIn	This counter represents the number of INVITE requests recei
SIPInviteRequestInForeign	This counter represents the current number of INVITE reques
SIPInviteRequestOut	This counter represents the number of INVITE requests sent
SIPInviteRequestOutForeign	This counter represents the current number of INVITE reques
SIPMessageRequestIn	This counter represents the number of MESSAGE requests re
SIPMessageRequestInForeign	This counter represents the current number of MESSAGE req

Counters	Counter Descriptions
SIPMessageRequestOutForeign	This counter represents the current number of MESSAGE reques
SIPNotifyRequestIn	This counter represents the number of NOTIFY requests receive
SIPNotifyRequestInForeign	This counter represents the current number of NOTIFY requests
SIPNotifyRequestOutForeign	This counter represents the current number of NOTIFY requests
SIPRegisterRequestIn	This counter represents the number of REGISTER requests recei
SIPRequestInForeign	This counter represents the current number of requests received
SIPRequestOutForeign	This counter represents the current number of requests sent direc
SIPRetransmits	This counter represents the number of retransmits executed by th
SIPSubscribeRequestIn	This counter represents the number of SUBSCRIBE requests rec
SIPSubscribeRequestInForeign	This counter represents the current number of SUBSCRIBE reque
SIPSubscribeRequestOutForeign	This counter represents the current number of SUBSCRIBE requ

Cisco Sync Agent

This object provides information about the number of errors that occur during synchronization. The following table contains information about the Cisco Sync Agent counter.

Table 72: Cisco Sync Agent Counter

Counter	Counter Description
NumberOfSyncErrors	This counter displays the number of errors that occur during synchronization. The counter resets to 0 when the Cisco sync agent is restarted. This counter is always 0 on the subscriber node.

Cisco XCP Auth Component

The following table contains information about Cisco XCP Authentication performance counters.

Table 73: Cisco XCP Auth Component Counters

Counter	Counter description
SASLPlainSuccess	This counter represents the total number of successful SASL plain authentication attempts.
SASLPlainFailed	This counter represents the total number of failed SASL plain authentication attempts.

Counter	Counter description
VtgTokenSuccess	This counter represents the number of successful vtg-token authentication attempts.
VtgTokenFailed	This counter represents the number of failed vtg-token authentication attempts.
FailedLicense	This counter represents the total number of failed authentication attempts due to no license.
FailedSASLCredentials	This counter represents the total failed SASL plain authentication attempts due to invalid username and password.
FailedTokenCredentials	This counter represents the total failed vtg-token authentication attempts due to invalid username and password.

Cisco XCP CM

The following table contains information about Cisco XCP Connection Manager (CM) performance counters.

Table 74: Cisco XCP CM Counters

Counter	Counter Description
CmConnectedSockets	This counter represents the number of connected sockets in the Web Connection Manager component.
CmSocketsAccepted	This counter represents the total number of accepted TCP sockets over the time interval.
CmSocketsClosed	This counter represents the total number of closed TCP sockets over the time interval.
CmXMPPStreamsClosedClientTCP	This counter represents the total number of XMPP streams closed due to closing TCP socket.
CmXMPPStreamsClosedDisconnect	This counter represents the total number of XMPP streams closed due to XMPP client signing out.
CmXMPPStreamsClosedSystemShutdown	This counter represents the total number of XMPP streams closed due to system shutdown.
CmXMPPStreamsClosedSeeOtherHost	This counter represents the total number of XMPP streams closed by IM and Presence server.
CmXMPPStreamsClosedStreamError	This counter represents the total number of XMPP streams closed due to XMPP stream error.
CmSocketOperationsPaused	This flag indicates if CM socket operations are paused (1) or not (0).

Counter	Counter Description
CmClientWorkerQueuesCount	This counter represents the current number of entries in all client processing queues.
CmClientWorkerQueuesProcessed	This counter represents the total number of entries from all client processing queues which are processed over the time interval.
CmClientSocketStreamWriteQueuesCount	This counter represents the current number of entries in all client XMPP stream write queues.
CmClientSocketStreamWriteQueuesProcessed	This counter represents the total number of entries from all client XMPP stream write queues which are processed over the time interval.
CmInFromClientCount	This counter represents the total number of all XMPP stanzas received from clients over the time interval.
CmInFromClientKBytes	This counter represents the total size (KB) of all XMPP stanzas received from clients over the time interval.
CmInFromClientKBytes	This counter represents the total size (KB) of all XMPP stanzas received from clients over the time interval.
CmOutToClientCount	This counter represents the total number of all XMPP stanzas sent to clients over the time interval.
CmOutToClientKBytes	This counter represents the total size (KB) of all XMPP stanzas sent to clients over the time interval.
CmInFromServerCount	This counter represents the total number of all XMPP stanzas received from XCP Router service over the time interval.
CmInFromServerKBytes	This counter represents the total size (KB) of all XMPP stanzas received from XCP Router service over the time interval.
CmOutToServerCount	This counter represents the total number of all XMPP stanzas sent to XCP Router service over the time interval.
CmOutToServerKBytes	This counter represents the total size (KB) of all XMPP stanzas sent to XCP Router service over the time interval.

Cisco XCP Component Stanza Traffic Counters

The following table provides information about Cisco XCP Component Stanza Traffic performance counters.

Table 75: Cisco XCP Component Stanza Traffic Counters

Counter	Counter description
CompStanzaNonChatMessagePacketsRecv	Non-chat message packets received by the component over the time interval.
CompStanzaNonChatMessagePacketsSent	Non-chat message packets sent from the component over the time interval.
CompStanzaXDBPacketsRecv	XDB packets received by the component over the time interval.
CompStanzaXDBPacketsSent	XDB packets sent from the component over the time interval.
CompJAXWorkerQueueCount	This counter represents the current number of entries in JAX connection processing queue.
CompJAXWorkerQueueProcessed	This counter represents the total number of entries from JAX connection processing queue processed over the time interval.
CmJAXSocketStreamWriteQueueCount	This counter represents the current number of entries in JAX socket stream write queue.
CmJAXSocketStreamWriteQueueProcessed	This counter represents the total number of entries from JAX socket stream write queue processed over the time interval.
CompStanzaErrorsSent	The number of error packets sent from the component over the time interval.
CompKBytesRecv	KBytes received by the component over the time interval.
CompKBytesSent	KBytes sent from the component over the time interval.
CompStanzaErrorsReceived	The number of error packets received by the component over the time interval.
CompStanzaChatMessagePacketsSent	Chat message packets sent from the component over the time interval.
CompStanzaChatMessagePacketsRecv	Chat message packets received by the component over the time interval.

Cisco XCP Jabberd Port Stanza Traffic

The following table contains information about the Cisco XCP Jabberd Port Stanza Traffic performance counters.

Table 76: Cisco XCP Jabberd Port Stanza Traffic

Counter	Counter description
JabberdPortStanzasFromRealm	This counter represents the total size (KB) of all XMPP stanzas received from the realm over the time period.
JabberdPortKBytesFromRealm	This counter represents the total number of XMPP stanzas sent to the realm over the time period.
JabberdPortStanzasToRealm	This counter represents the total number of XMPP stanzas sent to the realm over the time period.
JabberdPortKBytesToRealm	This counter represents the total size (KB) of all XMPP stanzas sent to the realm over the time period.

Cisco XCP JDS

The following table contains information about the Cisco XCP JDS performance counters.

Table 77: Cisco XCP JDS Counters

Counter	Counter description
JdsLDAPSuccess	This counter represents the total successful LDAP searches within the JDS component.
JdsLDAPFailed	This counter represents the total failed LDAP searches within the JDS component.
JdsInvalidRequests	This counter represents the number of requests rejected by JDS component.

Cisco XCP JSM

The following table contains information about the XCP JSM performance counters.

Table 78: Cisco XCP JSM Counters

Counter	Counter description
JsmOnlineUsers	This counter represents the current number of online users managed by the JSM.

Counter	Counter description
JsmSessionsEnded	This counter represents the number of IM sessions ended by the JSM over the time interval.
JsmStanzaNonChatMessagesIn	This counter represents the number of non-chat message stanzas sent by the JSM.
JsmStanzaNonChatMessagesOut	This counter represents the number of non-chat message stanzas received by the JSM.
JsmStanzaIQIn	This counter represents the number of iq stanzas sent by the JSM.
JsmStanzaIQOut	This counter represents the number of iq stanzas received by the JSM.
JsmStanzaErrorsIn	This counter represents the number of error stanzas sent by the JSM.
JsmStanzaErrorsOut	This counter represents the number of error stanzas received by the JSM.
JsmMTQsJSMCount	This counter represents the current number of entries in all MTQs from JSM thread pool entry queue.
JsmMTQsJSMProcessed	This counter represents the total number of entries from all MTQs from JSM thread pool entry queue processed over the time interval.
JsmMTQsJSMDBCount	This counter represents the current number of entries in all MTQs from JSM DB thread pool entry queue.
JsmMTQsJSMDBProcessed	This counter represents the total number of entries from all MTQs from JSM DB thread pool entry queue processed over the time interval.
JsmPresenceThrottlingMapAdded	This counter represents the total number of entries added to Presence Throttling map over the time interval.
JsmPresenceThrottlingPresenceSent	This counter represents the total number of presence packets sent by Presence Throttling over the time interval.
JsmPresenceThrottlingPresenceUsrgrpSent	This counter represents the total number of usergroup presence packets sent by Presence Throttling over the time interval.
JsmPresenceThrottlingMapSkipped	This counter represents the total number of entries from Presence Throttling map skipped over the time interval.

Counter	Counter description
JsmSessionsClient	This counter represents the number of CLIENT sessions active for the JSM.
JsmSessionsClientInactive	This counter represents the number of CLIENT sessions inactive for the JSM.
JsmSessionsComposed	This counter represents the number of COMPOSED sessions active for the JSM.
JsmSessionsComposedInactive	This counter represents the number of COMPOSED sessions inactive for the JSM.
JsmSessionsPhantom	This counter represents the number of PHANTOM sessions active for the JSM.
JsmSessionsHybrid	This counter represents the number of HYBRID sessions active for the JSM.
JsmSessionsCreated	This counter represents the number of IM sessions created by the JSM over the time interval.
JsmPresenceThrottlingMapSize	This counter represents the total number of entries from Presence Throttling map skipped over the time interval.
JsmPresenceThrottlingSemValue	This counter represents the current value of Presence Throttling burst semaphore.
JsmSessionsTotal	This counter represents the current number of non-composed IM sessions managed by the JSM.
JsmSessionsMaxTotalPtg	This counter represents the currently used percentage of maximum number of active non-composed IM sessions allowed for the JSM.
JsmStanzaChatMessagesIn	This counter represents the number of chat message stanzas sent by the JSM.
JsmStanzaChatMessagesOut	This counter represents the number of chat message stanzas received by the JSM.
JsmStanzaPresenceIn	This counter represents the number of presence stanzas sent by the JSM.
JsmStanzaPresenceOut	This counter represents the number of presence stanzas received by the JSM.
JsmUsrgrpTotalGroupsSubscribed	This counter represents the total number of groups subscribed.
JsmUsrgrpTotalPresenceSentToWatchers	This counter represents the total number of presence packets sent to watchers subscribed to groups.

Counter	Counter description
JsmUsrgrpTotalRosterLimitErrorSent	This counter represents the total number of roster limit error packets sent to watchers subscribed to a group.
JsmPresenceThrottlingAvgDelay	This counter represents the average delay of presence packets caused by Presence Throttling over the time interval.
JsmTempPresenceSubsCount	This counter represents the current number of active temporary presence subscriptions to all local users.
JsmTempPresenceSubsAdded	This counter represents the total number of temporary presence subscriptions to local users added over the time interval.
JsmRosterPresenceSubsCount	This counter represents the current number of presence subscriptions of all local users.
JsmRosterWatchersCount	This counter represents the current number of presence watchers of all local users.
JsmTempPresenceSubsRemoved	This counter represents the total number of temporary presence subscriptions to local users removed over the time interval.
JsmTempPresenceUpdatesSent	This counter represents the total number of temporary presence updates sent over the time interval.

Cisco XCP JSM DB Counters

The following table contains information about the Cisco XCP JSM DB performance counters.

Table 79: Cisco XCP JSM DB Counters

Counter	Counter description
JsmDBQueueAdded	This counter represents the number of JSM DB requests created during time interval.
JsmDBQueueForeignRealmAdded	This counter represents the number of JSM DB requests coming from non-local components during time interval.
JsmDBQueueRemoved	This counter represents the number of JSM DB requests processed during time interval.
JSMDBQueueSize	This counter represents the number of JSM DB requests processed during time interval.

Cisco XCP JSM IQ Namespaces

The following table contains information about the Cisco XCP JSM IQ Namespaces performance counters.

Table 80: Cisco XCP JSM IQ Namespaces

Counter	Counter description
JSM IQ Namespace	This counter represents the number of IQ stanzas by type handled by the JSM.

Cisco XCP JSM Session Counters

The following table contains information about the Cisco XCP JSM Session performance counters.

Table 81: Cisco XCP JSM Session Counters

Counter	Counter description
JsmSessionIQIn	This counter represents IQ packets received by JSM on a session.
JsmSessionIQOut	This counter represents IQ packets sent by JSM on a session.
JsmSessionMessagesIn	This counter represents message packets received by JSM on a session.
JsmSessionMessagesOut	This counter represents message packets sent by JSM on a session.
JsmSessionPresenceIn	This counter represents presence packets received by JSM on a session.
JsmSessionPresenceOut	This counter represents presence packets sent by JSM on a session.
JsmSessionRosterSize	This counter represents snapshot size of roster for a user.

Cisco XCP MA Basic

The following table contains information about the Cisco XCP Message Archiver Basic performance counters.

Table 82: Cisco XCP MA Basic Counters

Counter	Counter description
MaReceivedPackets	This counter represents the number of incoming messages archived by the message archiver component.

Counter	Counter description
MaSentPackets	This counter represents the number of outgoing messages archived by the message archiver component.
MaSuccessDBWrites	This counter represents the number of successful database writes to the message archiver component.
MaFailedDBWrites	This counter represents the number of failed database writes to the message archiver component.
MaPacketsDropped	This counter represents the number of dropped packets by the message archiver component.
MaDBQueueSize	This counter represents the number of packets the message archiver has pending to write to its database.

Cisco XCP MDM Counters

The following table contains information about the Cisco XCP MDM performance counters.

Table 83: Cisco XCP MDM Counters

Counter	Counter description
MDMBufferAvgQueuedTime	This counter represents the average time in seconds before MDM buffer is flushed.
MDMBufferFlushPacketCount	This counter represents the number of packets flushed in the last timeslice.
MDMBufferFlushes	This counter represents the total number of MDM buffer flushes.
MDMBufferFlushesLimitReached	This counter represents the total number of MDM buffer flushes due to reaching overall buffer size limit.
MDMQuietModeSessions	This counter represents the current number of sessions in quiet mode.
MDMSessions	This counter represents the current number of MDM enabled sessions.
MDMSilentModeSessions	This counter represents the current number of sessions in silent mode.

Cisco XCP MFT Counters

The following table contains information about the Cisco XCP MFT performance counters.

Table 84: Cisco XCP MFT Counters

Counter	Counter description
MFTFilesDownloaded	This counter represents the total number of files downloaded.
MFTFilesUploaded	This counter represents the total number of files uploaded.
MFTFilesDownloadedLastTimeslice	This counter represents number of files downloaded in the last timeslice.
MFTFilesUploadedLastTimeslice	This counter represents the number of files uploaded in the last timeslice.
MFTBytesDownloadedLastTimeslice	This counter represents the number of bytes downloaded in the last timeslice.
MFTBytesUploadedLastTimeslice	This counter represents the number of bytes uploaded in the last timeslice.

Cisco XCP Managed File Transfer

The following table contains information about the Cisco XCP Managed File Transfer performance counters.

Table 85: Managed File Transfer Counters

Counter	Counter description
MFTBytesDownloadedLastTimeslice	This counter represents the number of bytes downloaded during the last reporting interval (typically 60 seconds).
MFTBytesUpoadedLastTimeslice	This counter represents the number of bytes uploaded during the last reporting interval (typically 60 seconds).
MFTFilesDownloaded	This counter represents the total number of files downloaded.
MFTFilesDownloadedLastTimeslice	This counter represents the number of files downloaded during the last reporting interval (typically 60 seconds).
MFTFilesUploaded	This counter represents the total number of files uploaded.
MFTFilesUploadedLastTimeslice	This counter represents the number of files uploaded during the last reporting interval (typically 60 seconds).

Cisco XCP Push Counters

The following table contains information about the Cisco XCP Push performance counters.

Table 86: Cisco XCP Push Counters

Counter	Counter description
PushEnabledSessions	The current number of active PUSH-enabled client sessions. This gets decremented only when PUSH gets disabled or upon client session end.
PushEnableReqRcvd	The number of PUSH enable requests received by the IM and Presence server during the counter interval.
PushErrors	The number of PUSH errors received during the counter interval.
PushSentSilent	The number of messages sent to clients in silent mode. A PUSH-enabled client session moves to silent mode when the Jabber app on the iOS device goes to the background.
PushSentDisconn	The number of messages sent to clients in suspended state. A PUSH-enabled client session moves to suspended state when the Jabber app on the iOS device goes to the background and the network.

Cisco XCP Router

The following table contains information about the Cisco XCP Router performance counters.

Table 87: Cisco XCP Router Counters

Counter	Counter description
RouterNormalPackets	This counter represents the total number of normal packets handled by the Cisco XCP router.
RouterXdbPackets	This counter represents the total number of xdb packets handled by the Cisco XCP router.
RouterRoutePackets	This counter represents the total number of route packets handled by the Cisco XCP router.
RouterLogPackets	This counter represents the total number of log packets handled by the Cisco XCP router.
RouterMTQsMIOCount	This counter represents the current number of entries in all MTQs from MIO thread pool entry queue.

Counter	Counter description
RouterMTQsMIOProcessed	This counter represents the total number of entries from all MTQs from MIO thread pool entry queue processed over the time interval.
RouterMTQsDeliveryCount	This counter represents the current number of entries in all MTQs from Delivery thread pool entry queue.
RouterMTQsDeliveryProcessed	This counter represents the total number of entries from all MTQs from Delivery thread pool entry queue processed over the time interval.

Cisco XCP SIP S2S

The following table contains information about Cisco XCP SIP Server-to-Server (S2S) performance counters.

Table 88: Cisco SIP S2S counters

Counter	Counter description
SIPS2SIncomingDomains	This counter represents the total foreign domains with incoming subscriptions.
SIPS2SOutgoingDomains	This counter represents the total foreign domains with outgoing subscriptions.
SIPS2SSubscriptionsOut	This counter represents the number of active outgoing subscriptions.
SIPS2SSubscriptionsIn	This counter represents the number of active incoming subscriptions.
SIPS2SSubscriptionsPending	This counter represents the total pending SIP outgoing subscriptions.
SIPS2SNotifyIn	This counter represents the total number of SIP NOTIFY messages received.
SIPS2SNotifyOut	This counter represents the total number of SIP NOTIFY messages sent.
SIPS2SMessagesIn	This counter represents the total number of SIP MESSAGE messages received.
SIPS2SMessagesOut	This counter represents the total number of SIP MESSAGE messages sent.
SIPS2SByeIn	This counter represents the total number of SIP BYE messages received.
SIPS2SInviteIn	This counter represents the total number of SIP INVITE messages received.

Counter	Counter description
SIPS2SInviteOut	This counter represents the total number of SIP INVITE messages sent.

Cisco XCP S2S

The following table contains information about Cisco XCP Server-to-Server (S2S) performance counters.

Table 89: Cisco XCP S2S Counters

Counters	Counter description
S2SIncomingDomains	This counter represents the total foreign domains with incoming subscriptions.
S2SOutgoingDomains	This counter represents the total foreign domains with outgoing subscriptions.
S2SFailedDialbackIn	This counter represents the total number of failed incoming dialback attempts.
S2SFailedDialbackOut	This counter represents the total failed number of outgoing dialback attempts.

Cisco XCP Stream Management Counters

The following table contains information about the Cisco XCP Stream Management Counters performance counters.

Table 90: Cisco XCP Stream Management Counters

Counter	Counter description
JsmSMBuffersResendSize	This counter represents the current number of packets buffered in resend buffers for all sessions.
JsmResumedSessions	This counter represents the number of suspended sessions that were resumed over the time period.
JsmSuspendedSessions	This counter represents the current number of sessions in a suspended state.
JsmExpiredSessions	This counter represents the number of suspended sessions that were terminated due to SM timeout over the time period.
JsmSMBuffersResendSize	This counter represents the current number of packets buffered in resend buffers for all sessions.

Cisco XCP SDNS Counters

The following table contains information about the Cisco XCP SDNS performance counters.

Table 91: Cisco XCP SDNS Counters

Counter	Counter description
CacheLookupCount	This counter represents the number of SDNS cache lookups in the last time slice.
DatabaseLookupCount	This counter represents the number of SDNS database lookups in the last time slice.
CacheSize	This counter represents the current number of elements in the SDNS cache.

Cisco XCP TC

The following table contains information about Cisco XCP Text Conferencing (TC) performance counters.

Table 92: Cisco XCP TC Counters

Counter	Counter description
TcTotalRooms	This counter represents the total number of all types of text chat rooms.
TcAdhocRooms	This counter represents the total number of ad hoc text chat rooms.
TcPersistentRooms	This counter represents the total number of permanent text chat rooms.
TcCreatedRooms	This counter represents the total number of created text chat rooms.
TcDeletedRooms	This counter represents the total number of deleted text chat rooms.
TcMessagesIn	This counter represents the total number of group chat messages received.
TcMessagesOut	This counter represents the total number of group chat messages sent.
TcDirectedMessagesIn	This counter represents the total number of private and invite messages received.
TcMessagesPersisted	This counter represents the total number of messages archived to the external database.

Counter	Counter description
TcMessagesIgnored	This counter represents the total number of messages not archived to the external database.

Cisco XCP TC Room Counters

The following table contains information about the Cisco XCP TC Room performance counters.

Table 93: Cisco XCP TC Room Counters

Counter	Counter description
TCRoomNumOccupants	This counter represents number of occupants in MUC room.
TCRoomBytesSent	This counter represents number of bytes sent within MUC room.
TCRoomBytesRecv	This counter represents number of bytes received within MUC room.
TCRoomStanzasSent	This counter represents number of stanzas sent in MUC room.
TCRoomMsgPacketSent	This counter represents number of message packets sent within MUC room.
TCRoomMsgPacketsRecv	This counter represents number of message packets received within MUC room.
TCRoomPresencePacketsSent	This counter represents number of presence packets sent within MUC room.
TCRoomPresencePacketsRecv	This counter represents number of presence packets received within MUC room.
TCRoomIQPacketsSent	This counter represents number of IQ packets sent within MUC room.
TCRoomIQPacketsRecv	This counter represents number of IQ packets received within MUC room.

Cisco XCP WebCM

The following table contains information about the Cisco XCP Web Connection Manager performance counters.

Table 94: Cisco XCP WebCM Counters

Counter	Counter description
WebCMConnectedSockets	This counter represents the number of connected sockets in the Web Connection Manager component.
WebCMFailedRequests	This counter represents the number of failed requests in the Web Connection Manager component.

Cisco XCP XDB Tracker Counters

The following table contains information about the Cisco XCP XDB Tracker performance counters.

Table 95: Cisco XCP XDB Tracker Counters

Counter	Counter description
JsmXDBTrackerQueueForeignRealmAdded	This counter represents the number of JSM XDBTracker requests coming from non-local components during time interval.
JsmMODExternalXDBTrackerQueueSize	This counter represents the current number of sent JSM Mod External XDBTracker requests pending response.
JsmMODExternalXDBTrackerQueueAdded	This counter represents the number of JSM Mod External XDBTracker requests sent during time interval.
JsmMODExternalXDBTrackerQueueRemoved	This counter represents the number of JSM Mod External XDBTracker requests processed during time interval.
JsmMODExternalXDBTrackerQueueForeignRealmAdded	This counter represents the number of JSM Mod External XDBTracker requests coming from non-local components during time interval.
JsmXDBTrackerQueueAdded	This counter represents the number of JSM XDBTracker requests sent during time interval.
JsmXDBTrackerQueueForeignRealmAdded	This counter represents the number of JSM XDBTracker requests coming from non-local components during time interval.
JsmXDBTrackerQueueRemoved	This counter represents the number of JSM XDBTracker requests processed during time interval.

Counter	Counter description
JsmXDBTrackerQueueSize	This counter represents the current number of sent JSM XDBTracker requests pending response.

Cisco Unity Connection Counters

CUC Data Store

The CUC Data Store object provides information about registered database usage by Cisco Unity Connection. The following table contains information about CUC Data Store counters.

Table 96: CUC Data Store

Counters	Counter Descriptions
Allocated Memory [kb]	Amount of database server virtual-address space [in kilobytes].
Database Connections	Total number of connections to the database server.
Disk Reads	Total number of disk read operations for all data chunks (rows) in the last 30 seconds.
Disk Reads/second	Number of read operations from the disk per second.
Disk Writes	Number of write operations to the disk in the last 30 seconds.
Disk Writes/second	Number of write operations to the disk per second.
Shared Memory [kb]	Amount of database server shared memory used [in kilobytes].

CUC Data Store: Databases

The CUC Data: Databases object provides information about the databases that Cisco Unity Connection uses.

Table 97: CUC Data Store: Databases

Counters	Counter Descriptions
Disk Reads/chunk	Number of read operations for the selected data chunk
Disk Writes/chunk	Number of write operations for the selected data

CUC Digital Notifications

The CUC Digital Notifications object provides information about the total number of SMS and SMTP notifications. The following table contains information about CUC Digital Notification counters.

Table 98: CUC Digital Notifications

Counters	Counter Descriptions
SMS Notifications Failed	The total number of SMS notifications failing to connect.
SMS Notifications Total	The total number of SMS notifications sent to subscribers by Cisco Unity Co
SMTP Notifications Total	The total number of SMTP notifications that Cisco Unity Connection sent to su
HTML Notifications with Summary of voice messages	The counter to maintain count of summary notifications.
HTML Notifications with Summary of voice messages in Last One Minute	The counter to maintain count of summary notifications sent in last one mi
Scheduled Notifications Total	The counter to maintain count of scheduled summary notifications sent.
Scheduled Notifications in Last One Minute	The counter to maintain count of scheduled summary notifications sent in la
Scheduled Notifications dropped due to Parent Schedule off	The counter to maintain count of scheduled summary notifications dropped because the parent schedule was turned off.
Scheduled Notifications dropped due to Parent Schedule off in Last One Minute	The counter to maintain count of scheduled summary notifications dropped in last one minute because the parent schedule was turned off.
Missed Call Notifications Total	The total number of missed call notifications sent fromCisco Unity Connec

CUC Directory Services

The CUC Directory Services object provides information about the performance of the directory services that Cisco Unity Connection uses.

The Directory Search Duration Average [s] counter represents the average time [in seconds] to complete a directory search request for the Cisco Unity Connection server.

CUC Feeder

The CUC Feeder object keeps a count of total requests processed by the Feeder. The following table contains information about CUC Feeder counters.

Counters	Counter Descriptions
Total objects requests processed	The total number of HTTP[S]/CCI objects requests processed by Feeder.
Objects requests processed in last 15 minutes	The total number of HTTP[S]/CCI objects requests processed by Feeder in last 15 minutes.

Counters	Counter Descriptions
Total object requests processed	The total number of HTTP[S]/CCI object requests processed by Feeder.
Object requests processed in last 15 minutes	The total number of HTTP[S]/CCI object requests processed by Feeder in last 15 minutes.

CUC Mailbox Sync

The Mailbox Sync service synchronizes messages between Unity Connection and Exchange.

The following table contains information about Mailbox Sync counters.

Counters	Counter Description
Active thread count	Cisco Unity Connection maintains threads for synchronization of voicemail from Cisco Unity Connection to Exchange server and vice-versa. At any moment, this counter specifies the number of threads that are actively in use for voicemail synchronization.
Background queue size	Mailbox sync has three types of priority queues: Background, Normal, and Time-Sensitive. Background queue is the lowest priority queue. This queue has items that are scheduled because of background re-synchronization of each mailbox hourly.
Normal queue size	Normal queue has moderate priority. This queue has items that are scheduled because of messaging operation (such as message CREATE, READ, UNREAD, DELETE) performed by user or any configuration update by administrator on Unified Messaging page on Cisco Unity Connection Administration.
Time sensitive queue size	Time sensitive queue has highest priority. This queue has such items that are scheduled because of keep-alive message sent by Cisco Unity Connection to Exchange server to keep subscription alive. This is applicable for 2003 Exchange server only.
Total connection errors	It specifies the number of times the CuMbxSync process fails to retrieve or update some data from database.
Total Mailbox Adds	It specifies the number of times a user mailbox has been setup for subscription. Any communication error between Unity Connection and Exchange, results in user mailbox remove and re-add.

Counters	Counter Description
Total Mailbox Removes	It specifies the number of times a user mailbox has been setup for un-subscription. Any communication error between Unity Connection and Exchange, results in user mailbox remove and re-add.
Total Resyncs	It specifies the total number of times user mailbox is resynchronized with Exchange server. Cisco Unity Connection does background resynchronization for all the user mailboxes hourly.
Total Retries	Whenever there is a communication failure between Cisco Unity connection and Exchange server, Unity Connection does mailbox synchronization retry for particular user mailbox. This counter specifies the count of such occurrences.
Total Work Items	It specifies number of times any messaging operation, such as CREATE, READ, UNREAD, and DELETE, has been performed on any user mailbox.

CUC Mailbox Sync on Gmail Server

Google Workspace service synchronizes messages between Unity Connection and mailbox on Gmail server. The following table contains information about its counters.

Counters	Counter Description
Active Thread Count From Gmail To Connection	This counter will record the count of currently active threads performing synchronization from Gmail server to Unity Connection
Active Thread Count From Connection to Gmail	This counter will record the count of currently active threads performing synchronization from Unity Connection to Gmail server.
Outstanding Request of Gmail to Connection	This counter will record the count of queue size for messages which are going to be synchronized from Gmail server to Unity Connection at specific point of time.
Outstanding Request of Connection to Gmail	This counter will record the count of queue size for messages which are going to be synchronized from Unity Connection to Gmail server at specific point of time.
Total Database Connection Errors	This counter will record all the operations which failed in performing database functionality while synchronizing the message.

Counters	Counter Description
Total HTTPs Requests	This counter will record all the HTTP requests sent to Gmail server.
Total HTTPs Failure	This counter will record all the errors occurred in HTTP requests.
Total Mailbox Adds	This counter will record the total count of Unified Messaging Accounts (UMA) added on the system. (Removing a UMA will not decrease its value)
Total Mailbox Removes	This counter will record the total count of Unified Messaging Accounts(UMA) removed from system. (Adding a UMA will not decrease its value)
Total Resyncs	This counter will record the total count of resynchs done on the system.
Total Retries	This counter will record the total count of retries done for the message to be synchronized.
Read Message on Connection	This counter will record the count for messages marked read on Unity Connection in response to synchronization from Gmail server.
Unread Message on Connection	This counter will record the count for messages marked unread on Unity Connection in response to synchronization from Gmail server.
Delete Message on Connection	This counter will record the count for messages marked delete on Unity Connection in response to synchronization from Gmail server.
Create Message on Connection	This counter will record the count for messages created on Unity Connection in response to synchronization from Gmail server.
Read Message on Gmail	This counter will record the count for messages marked read on Gmail server in response to synchronization from Unity Connection.
Unread Message on Gmail	This counter will record the count for messages marked unread on Gmail server in response to synchronization from Unity Connection.
Delete Message on Gmail	This counter will record the count for messages marked delete on Gmail server in response to synchronization from Unity Connection.
Create Message on Gmail (Inbox Folder)	This counter will record the count for messages created on mailbox on Gmail server in response to synchronization from Unity Connection.

Counters	Counter Description
Create Message on Gmail (Sent Folder)	This counter will record the count for messages created on mailbox on Gmail server(Sent) in response to synchronization from Unity Connection.

CUC Message Store

The CUC Message Store object provides information about the performance of the Cisco Unity Connection message store. The following table contains information about CUC Message Store counters.

Table 99: CUC Message Store

Counters	Counter Descriptions
Bad Mail Total	Total number of messages sent to the Bad Mail folder since the last restart o server.
Delivery Receipts Total	Total number of delivery receipts since the last restart of the MTA server.
Incoming Recalls	Number of incoming requests to recall local copies of messages initiated by senders on other network locations.
Intersite Messages Delivered Per Minute	Number of intersite messages delivered in the last minute.
Intersite Messages Delivered Total	Total number of intersite messages delivered since the last restart of the M
Intersite Messages Received Per Minute	Number of intersite messages received in the last minute.
Intersite Messages Received Total	Total number of intersite messages received since the last restart of the MT
Intersite Messages Total	Total number of intersite messages that have been delivered and received s last restart of the MTA server.
Local Recalls	Number of message recalls initiated by local senders on this server.
Message Size Average [kb]	The average size of the MTA at each sample in kilobytes.
Messages Delivered Total	Total number of messages delivered since the last restart of the MTA serve
Messages Received Per Minute	Total number of messages received Per Minute by MTA.
Messages Received Total	Total number of messages received since the last restart of the MTA server.
Non-delivery Receipts Total	Total number of non-delivery receipts since the last restart of the MTA serv
Number of Items Recalled	Total number of message recalls. This number includes each individual cop message that was sent to multiple recipients, so this number could be much l the Total Recalls, Local and Remote performance counter.
Queued Messages Current	The number of messages currently queued in the MTA.
Read Receipts Total	Total number of read receipts since the last restart of the MTA server.

Counters	Counter Descriptions
Retries Total	Total number of retries since the last restart of the MTA server.
Total dispatch message folder items delivered	Total number of dispatch messages that have been delivered to individu mailboxes since the MTA started. This number includes a count of each copy of a message sent to multiple recipients.
Total dispatch messages accepted	Total number of dispatch messages that have been accepted since the las MTA server
Total dispatch messages delivered	Total number of dispatch messages that have been delivered since the M This number includes each message just once, regardless of the number
Total dispatch message items rejected	Total number of individual copies of dispatch messages that have been d the last restart of the MTA server.
Total dispatch messages removed due to acceptance	Total number of dispatch messages that have been removed from user m to the message being accepted by another user since the last restart of th
Total recalls, local and remote	Total number of message recalls initiated by local and remote senders. T should be equal to the total of Incoming Recalls and Local Recalls perfo counters.
VPIM Message Decode Duration Average [s]	The average time [in seconds] to decode voice messages in MIME format format.
VPIM Message Encode Duration Average [s]	The average time [in seconds] to encode voice messages to MIME form
VPIM Messages Delivered Per Minute	The number of VPIM messages that the Cisco Unity Connection Messa delivered within a minute.
VPIM Messages Delivered Total	The total number of VPIM messages that the Cisco Unity Connection M delivered.
VPIM Messages Received Per Minute	The number of VPIM messages that the Cisco Unity Connection Messa received per minute.
VPIM Messages Received Total	The total number of VPIM messages that the Cisco Unity Connection M received.
VPIM Messages Total	The total number of VPIM messages that the Cisco Unity Connection M processed.
Messages Undelivered Mailbox Quota Full Notification Total	The total number of missed call notification sent when mailbox quota is
Video Messages Delivered Total	The total number of video messages delivered since the last restart of the
Video Messages Delivered Per Minute	The total number of video messages delivered per minute since the last MTA server.
Video Messages Processed by MTA Total	The total number of video messages processed (both successful and uns the MTA server since the last restart of the server.

Counters	Counter Descriptions
Video Messages Processed by MTA Per Minute	The total number of video messages processed (both successful and unsucc the MTA server per minute since the last restart of the server.

CUC Message Store: Databases

The CUC Message Store: Databases object provides information about the message store database that Cisco Unity Connection uses.

The Messages Delivered Per Message Store counter represents the total number of messages that were delivered per message store since the last restart of the MTA server.

CUC Personal Call Transfer Rules

The CUC Personal Call Transfer Rules object provides information about the numbers and usage of the personal call transfer rules (PCTR). The following table contains information about CUC Personal Call Transfer Rules counters.

Table 100: CUC Personal Call Transfer Rules

Counters	Counter Descriptions
Applicable Rule Found	Personal call transfer rule (PCTR) call resulted in rule processing, and an a transfer rule is found.
Destinations Tried	Number of destinations tried while transfer rules were applied.
PCTR Calls	Calls that are subject to personal call transfer rule (PCTR) processing: user COS is enabled for PCTR, user is a Unified Communications Manager use not disabled PCTR.
Rules Evaluated	Number of rules that are evaluated during rule processing in a personal call rule (PCTR) call.
Subscriber Reached	Number of times that a subscriber was reached while transfer rules were ap
Transfer Failed	Number of times that Cisco Unity Connection fails to transfer a call to a de while personal call transfer rules were applied. Transfer failures include all except when the called destination is connected, busy, or RNA or times out hanging up during a transfer gets considered a transfer failure.
Voicemail Reached	Number of times that voice mail was reached while transfer rules were app

CUC Phone System

The CUC Phone System object provides information about the performance of the phone system integration. The following table contains information about CUC Phone System counters.

Table 101: CUC Phone System

Counters	Counter Descriptions
Call Count Current	The current number of incoming and outgoing calls to the Cisco Unity server.
Call Count Total	The total number of incoming and outgoing calls to the Cisco Unity Conn
Call Duration Average [s]	The average duration [in seconds] of incoming and outgoing calls from th Connection server.
Call Duration Total [s]	The total duration [in seconds] of incoming and outgoing calls from the Connection server.
Calls Unanswered Total	The total number of unanswered calls on the Cisco Unity Connection se
Incoming Calls CFB Current	The current number of incoming calls that were received as Call Forwa
Incoming Calls CFB Total	The total number of incoming calls that were received as Call Forward
Incoming Calls CFNA Current	The current number of incoming calls that were received as Call Forwar
Incoming Calls CFNA Total	The total number of incoming calls that were received as Call Forward
Incoming Calls Current	The current number of incoming calls.
Incoming Calls Direct Current	The current number of incoming calls that were received as direct calls.
Incoming Calls Direct Total	The total number of incoming calls that were received as direct calls.
Incoming Calls Duration Average [s]	The average duration [in seconds] of all incoming calls to the Cisco Unit server.
Incoming Calls Duration Total [s]	The total duration [in seconds] of all incoming calls to the Cisco Unity server.
Incoming Calls No Info Total	The total number of incoming calls without integration information.
Incoming Calls Total	The total number of incoming calls.
Message Notification Duration Average [s]	The average time [in seconds] to complete all message notifications fro Unity Connection server.
Message Notification Duration Total [s]	The total time [in seconds] to complete all message notifications from th Connection server.
Message Notifications Failed	The total number of message notifications that failed to connect to a destin
Message Notifications Total	The total number of message notifications that Cisco Unity Connection subscribers.
MWI Request Duration Average [ms]	The average duration [in milliseconds] of all MWI requests from the Ci Connection server.

Performance Counters and Alerts

Counters	Counter Descriptions
MWI Request Duration Total [ms]	The total duration [in milliseconds] of all MWI requests from the Cisco Un Connection server.
MWI Requests Failed Total	The total number of MWI requests that failed to connect to a destination nu complete MWI operation.
MWI Requests Total	The total number of MWI requests that Cisco Unity Connection sent.
Outgoing Calls Duration Average [s]	The average duration [in seconds] of all outgoing calls from the Cisco Unity C server.
Outgoing Calls Duration Total [s]	The total duration [in seconds] of all outgoing calls from the Cisco Unity C server.
Outgoing Calls Release Transfers Completed	The number of completed release transfers from the Cisco Unity Connectio
Outgoing Calls Release Transfers Failed	The number of release transfers from the Cisco Unity Connection server tha connect to a destination number.
Outgoing Calls Release Transfers Total	The total number of release transfers that were attempted from the Cisco U Connection server.
Outgoing Calls Supervised Transfers Completed	The number of completed supervised transfers from the Cisco Unity Connect
Outgoing Calls Supervised Transfers Dropped	The number of supervised transfers from the Cisco Unity Connection server dropped while in progress.
Outgoing Calls Supervised Transfers Failed	The number of supervised transfers from the Cisco Unity Connection server to connect to a destination number.
Outgoing Calls Supervised Transfers Total	The total number of supervised transfers from the Cisco Unity Connection
Outgoing Calls Transfers Total	The total number of release and supervised transfers that Cisco Unity Conn attempted.
Pager Notifications Duration Average [s]	The average time [in seconds] to complete all pager notifications from the C Connection server.
Pager Notifications Duration Total [s]	The total time [in seconds] to complete all pager notifications from the Cis Connection server.
Pager Notifications Failed	The total number of pager notifications that failed to connect to a destinatio
Pager Notifications Total	The total number of pager notifications that Cisco Unity Connection sent to su
Port Idle Duration [s]	The total time [in seconds] that any port remains idle between incoming ca Cisco Unity Connection server.
Port Idle Duration Average [s]	The average time [in seconds] that any port remains idle between incoming the Cisco Unity Connection server.

Counters	Counter Descriptions
Ports Idle Current	The current number of integration ports that are not in use by the Cisco Connection server.
Ports In Use Current	The current number of integration ports that are in use by the Cisco Unit server.
Ports Locked	The current count of the ports that no longer respond or are otherwise u Cisco Unity Connection.
Missed Call Total	The total number of missed call notifications triggered by theCisco Unit server.

CUC Phone System: Ports

The CUC Phone System: Ports object provides information about the voice messaging ports on Cisco Unity Connection. The following table contains information about CUC Phone System: Ports counters.

Table 102: CUC Phone System: Ports

Counters	Counter Descriptions
Port Calls	The total number of calls that were received on this port since the Cisco Connection server was last restarted. This includes all types of calls: In MWI dialouts, Notification dialouts, TRAP dialouts, and VPIM dialout
Port Idle Percent	The distribution percentage of idle ports on the Cisco Unity Connection
Port Usage Duration Average [s]	The average time [in seconds] that a port has been actively processing c
Port Usage Duration Total [s]	The total time [in seconds] that a port has been actively processing calls
Port Usage Percent	The distribution percentage of calls into ports on the Cisco Unity Conne

CUC Replication

The CUC Replication object provides information about the replication for Cisco Unity Connection redundancy. The following table contains information about CUC Replication counters.

Table 103: CUC Replication

Counters	Counter Descriptions
File Replication Latency [s]	How long file exists before replication starts.
File Replication Latency Max [s]	Maximum file replication latency since the service started.
File Transfer Rate [kbytes/s]	Transfer rate for each replicated file.
Files Replicated Total	Number of files replicated since the service started.

Counters	Counter Descriptions
Transfer Rate [bytes/s]	Number of bytes transferred each second.

CUC Replicator: Remote Connection Locations

The CUC Replicator: Remote Connection Locations object provides information about replication with remote Connection locations. The following table contains information about CUC Replicator: Remote Connection Locations counters.

Table 104: CUC Replicator: Remote Connection Locations

Counters	Counter Descriptions
Dependencies Requests Received	The number of replication dependencies requested received from the Conn location.
Dependencies Requests Sent	The number of replication dependencies requests sent to the Connection lo
Message Receive Failures	The number of replication messages from this Connection location that we received because of failures.
Message Send Failures	The number of replication messages to the Connection location that were n because of failures.
Messages Received	The number of replication messages received from the Connection location
Messages Sent	The number of replication messages sent to the Connection location.
NDR Messages Received	The number of replication NDR messages received from the Connection lo
USN Requests Received	The number of USN request received from the Connection location. This u indicates that a USN timeout occurred on the remote node.

Connection REST Tomcat Connector

The Tomcat Hypertext Transport Protocol (HTTP) and HTTP Secure (HTTPS) Connector object provides information about Tomcat connectors.

Connection Rest Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when VMREST requests of application are accessed. The Secure Socket Layer (SSL) status of VMREST request URL's provide the basis for instance name for each Rest Tomcat Connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.

The following table contains information about the Connection Rest Tomcat connector counters.

Counter	Counter Description
Errors	The total number of HTTP errors (for example, `401 Unauthorized`) that the connector encountered.

Counter	Counter Description
MBytesReceived	The amount of data that the connector received.
MBytesSent	The amount of data that the connector sent.
Requests	The total number of request that the connector handled.
ThreadsTotal	The current total number of request processing threads, including available and in-use threads, for the connector.
ThreadsMax	The maximum number of request processing threads for the connector. Each incoming VMREST request requires a thread for the duration of that request. If more simultaneous requests are received than the currently available request processing threads can handle, additional threads are created up to the configured maximum shown in this counter. If still more simultaneous requests are received, they accumulate within the server socket that the connector created, up to an internally specified maximum number. Any further simultaneous requests receive connection refused messages until resources are available to process them.
ThreadsBusy	This counter represents the current number of busy/in-use request processing threads for the connector.

Connection REST Tomcat JVM

The Cisco Tomcat Java Virtual Machine (JVM) object provides information about the pool of common resource memory used by VMREST requests URL's. The dynamic memory block stores all objects that Tomcat and its VMREST requests create.

The following table contains information about the Connection REST Tomcat JVM counters.

Counters	Counter Description
KBytesMemoryFree	The amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine. When the amount of free dynamic memory is low, more memory is automatically allocated, and total memory size (represented by the KbytesMemoryTotal counter) increases but only up to the maximum (represented by the KbytesMemoryMax counter). You can determine the amount of memory in use by subtracting KBytesMemoryFree from KbytesMemoryTotal.

Counters	Counter Description
KBytesMemoryMax	The amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine.
KBytesMemoryTotal	The current total dynamic memory block size, including free and in-use memory, of Tomcat Java Virtual Machine.

Connection REST Tomcat Web Application

Cisco Rest Tomcat Web Application object provides information about how to run VMREST request URL's.

VMREST request URL's provide the basis for instance name for each Rest Tomcat Web Application, as explained in the following examples:

- Cisco Unified Communications Manager Administration (https://<IP Address>:8443/ccmadmin) is identified by ccmadmin.
- Cisco Unified Serviceability (https://<IP Address>:8443/ccmservice) is identified by ccmservice.
- Cisco Unified Communications Manager User Options (https://<IP Address>:8443/ccmuser) is identified by ccmuser.
- Cisco Unity Connection Administration (https://<IP Address>:8443/cuadmin) is identified by cuadmin.
- URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), are identified by _root.

The following table contains information on the Connection Rest Tomcat Web Application counters.

Counters	Counter Description
Errors	The total number of HTTP errors (for example, 401 Unauthorized) that a Unified Communications Manager-related or Cisco Unity Connection-related web application encounters.
Requests	The total number of VMREST requests that the web application handles. Each time that a web application is accessed, its Requests counter increments accordingly.
SessionsActive	The number of active or in use sessions in the web application.

CUC Sessions: Authz Server

Table 105: CUC Sessions: Authz Server

Counters	Counter Description
CUC Authz Total Validation Requests	Total Number of Authz validation requests.
CUC Authz Successful Validation Requests	Total Number of successful Authz validations.

Counters	Counter Description
CUC Authz Failed Validation Requests	Total Number of failed Authz validations.
CUC Authz Total Validation Requests in Last minute	Total Number of Authz validations in Last minute.
CUC Authz Successful Validation Requests in Last minute	Total Number of successful Authz validations in last minute.
CUC Authz Failed Validation Requests in Last minute	Total Number of failed Authz validations in last minute.

CUC Sessions: Calendar Access

The CUC Sessions: Calendar Access object provides information about the Cisco Unity Connection calendar integration. The following contains information about CUC Sessions: Calendar Access counters.

Table 106: CUC Sessions: Calendar Access

Counters	Counter Descriptions
Connections To Exchange Failure - Total	Total number of Exchange connection failures.
Connections To MP Failure - Total	Total number of MeetingPlace connection failures.
Exchange Requests - Total	Total number of Exchange calendar requests.
Exchange Response Time [ms] - Current	Current Exchange Response Time in milliseconds.
Meeting Join Request - Total	Total number of requests to join the meeting.
MP Request - Total	Total number of MeetingPlace calendar requests.
MP Response Time [ms] - Current	Current MeetingPlace Response Time in milliseconds.

CUC Sessions: E-Mail Access

The CUC Sessions: E-mail Access object provides information about e-mail voice sessions. The following table contains information about CUC Sessions: E-mail Access counters.

Table 107: CUC Sessions: E-Mail Access

Counters	Counter Descriptions
Messages Read - Total	The total number of e-mail messages that were read since the last restart o Connection.
Session Duration Average [ms]	The average duration [in milliseconds] of all e-mail sessions as measured basis.
Session Duration Total [ms]	The total duration [in milliseconds] of all e-mail sessions as measured o basis.

Counters	Counter Descriptions
Sessions - Current	The number of active e-mail voice sessions.
Sessions - Total	The total number of e-mail voice sessions since the last restart of Cisco Un Connection.

CUC Sessions: IMAP Server

The CUC Sessions: IMAP Server object provides information about the IMAP server. The following table contains information about CUC Sessions: IMAP Server counters.

Table 108: CUC Sessions: IMAP Server

Counters	Counter Descriptions
Commands per minute	The number of IMAP commands per minute.
Connection Length Average [s]	The average duration [in seconds] of the connections to the IMAP server in th minute.
Current IDLE Sessions	The number of idle sessions on the IMAP server.
Errors Total	The total number of IMAP errors that the IMAP server returned since the la of the IMAP server.
EXAMINE Requests Total	The total number of EXAMINE requests to the IMAP server since the last the IMAP server.
Failed Login Requests Total	The total number of failed LOGIN requests to the IMAP server since the la of the IMAP server.
FETCH Requests Total	The total number of FETCH requests to the IMAP server since the last rest IMAP server.
Login Requests Total	The total number of LOGIN requests to the IMAP server since the last rest IMAP server.
Logout Requests Total	The total number of LOGOUT requests to the IMAP server since the last res IMAP server.
Messages Read Total	The total number of IMAP FETCH commands that have returned the body message since the IMAP was last restarted.
Messages Read/hour	The number of IMAP FETCH commands in the previous hour that returned of a message.
Messages/fetch Average	Average number of messages that the IMAP FETCH command returned.
NOOP Requests Total	The total number of NOOP requests to the IMAP server since the last resta IMAP server.
Response Time [ms]	The response time [in milliseconds] for IMAP commands.

Counters	Counter Descriptions
SEARCH Requests Total	The total number of SEARCH requests to the IMAP server since the las IMAP server.
Socket Connections Current	The number of active socket connections to the IMAP server.
Socket Connections Total	The total number of socket connections that have been made to the IMA it was last restarted.
STARTTLS Requests Total	The total number of STARTTLS requests to the IMAP server since the the IMAP server. This counter also increments when clients connect to t port directly.
STATUS Requests Total	The total number of STATUS requests to the IMAP server since the las IMAP server.
TLS Connections Current	The number of active Transport Layer Security connections to the IMA
TLS Errors Total	The total number of failed TLS connections to the IMAP server since t of the IMAP server.
Unsolicited Notify Response Time Average [ms]	Average Unsolicited Notify Response Time [in milliseconds] for the IM
Unsolicited Notify Responses Total	Total number of Unsolicited Notify Responses that the IMAP server mad last restarted.

CUC Sessions: RSS

The CUC Sessions: RSS object provides information about RSS sessions. The following table contains information about CUC Sessions: RSS counters.

Table 109: CUC Sessions: RSS

Counters	Counter Descriptions
RSS Messages Offered Total	The total number of RSS messages that were offered for streaming.
RSS Messages Streamed Total	The total number of RSS messages that the Cisco Unity Connection ser
RSS Sessions Current	The current number of RSS sessions.
RSS Sessions Total	The total number of RSS sessions.

CUC Sessions: SMTP Server

The CUC Sessions: SMTP Server object provides information about SMTP server sessions. The following table contains information about CUC Sessions: SMTP Server counters.

Table 110: CUC Sessions: SMTP Server

Counters	Counter Descriptions
Total Delivered Messages	The number of SMTP messages that were delivered since the start of the sy
Total Messages	The number of SMTP messages delivered or received since the start of the
Total Received Messages	The number of SMTP messages that were received since the start of the sys

CUC Sessions: SpeechView Processor

The CUC Sessions: SpeechView Processor object provides information about the SpeechView Processor service. The following table contains information about CUC Sessions: SpeechView Processor counters.

Table 111: CUC Sessions: SpeechView Processor

Counters	Counter Descriptions
Average wait time	The average time it takes to receive successful transcriptions from the extern
Total failures	The total number of failed transcriptions since the last restart of the Speech Processor service.
Total timeouts	The total number transcriptions that timed out since the last restart of the Sp Processor service.
Transcribed messages	The total number successful transcriptions since the last restart of the Spee Processor service.

CUC Sessions: TRaP

The CUC Sessions: TRaP object provides information about telephone record and playback (TRaP) sessions. The following table contains information about CUC Sessions: TRaP counters.

Table 112: CUC Sessions: TRaP

Counters	Counter Descriptions
Reverse TRaP Session Duration Average [s]	The average duration [in seconds] of all reverse TRaP sessions.
Reverse TRaP Session Duration Total [s]	The total duration [in seconds] of all reverse TRaP sessions.
Reverse TRaP Sessions Current	The current number of active reverse TRaP sessions.
Reverse TRaP Sessions Total	The total number of reverse TRaP sessions since the last start of Cisco Uni Connection.
TRaP Session Duration Average [s]	The average duration [in seconds] of all TRaP sessions.
TRaP Session Duration Total [s]	The total duration [in seconds] of all TRaP sessions.

Counters	Counter Descriptions
TRaP Sessions Current	The current number of active TRaP sessions.
TRaP Sessions Total	The total number of TRaP sessions since the last start of Cisco Unity C

CUC Sessions: TTS

The CUC Sessions: TTS object provides information about text-to-speech (TTS) sessions. The following table contains information about CUC Sessions: TTS counters.

Table 113: CUC Sessions: TTS

Counters	Counter Descriptions
Session Duration Average [s]	The average duration [in seconds] of all TTS sessions.
Session Duration Total [s]	The total duration [in seconds] of all TTS sessions.
Sessions Current	The current number of active TTS voice sessions.
Sessions Total	The total number of TTS voice sessions since the last start of Cisco Unit

CUC Sessions: Unified Client

The CUC Sessions: Unified Client object provides information about the Unified Client for Cisco Unity Connection.

The Connections Total counter represents the total number of Unified Client IMAP requests.

CUC Sessions: Video

CUC Sessions Video: Video session object provides information about video sessions with video server. The following table contains information about CUC Sessions: Video

Table 114: CUC Sessions: Video

Counters	Counter Descriptions
Audio calls Negotiated Total	The total number of Audio calls negotiated despite video offer.
Audio Calls Negotiated In Last One Minute	The total number of audio calls negotiated despite video offer in last one minute.
Outgoing Video calls Release Transfer	The total number of outgoing video calls transferred as Release to Switch.
Supervise Transfer Calls Total	The total number of Supervise transfers initiated from video calls since the last restart of Cisco Unity Connection.

Counters	Counter Descriptions
Video calls downgraded to Audio Total	The total number of video calls downgraded to audio since the last restart of Unity Connection.
Video calls downgraded to Audio In Last One Minute	The total number of video calls downgraded to audio in last one minute.
Video calls downgraded with prompt total	Total number of video calls downgraded with prompt "Video services are not available using audio only for duration of this call".
Video calls downgraded with prompt in Last One Minute	Total number of video calls downgraded with prompt "Video services are not available using audio only for duration of this call" in last minute.
Video Sessions Total	The total number of video session requests sent from Unity Connection to Video Server.
Video Sessions Current	The total number of current video session requests sent from Unity Connection to Video Server.
Video Session Playbacks Total	The total number of video session playbacks since the last restart of Cisco Unity Connection.
Video Session Playbacks Current	The total number of current video session playbacks.
Video Media File Playbacks Total	The total number of image playbacks from video server since the last restart of Unity Connection.
Video Media File Playbacks Current	The current number of Video Media File playbacks from video server.
Video Recordings Total	The total number of Video Recordings saved at video server since the last restart of Unity Connection.
Video Recordings Current	The current number of Video Recordings saved at video server.
Video Playback Completed Events from MS Total	The total number of Video Playback completed events from video server since the last restart of Unity Connection.
Video Playback Completed Events from MS In Last One Minute	The total number of Video Playback completed events from video server since last one minute.
Video Keep Alive Total	The total number of Keep Alive sent by Unity Connection to video server since the last restart of Unity Connection.
Video Keep Alive In Last One Minute	The total number of Keep Alive sent by Unity Connection to video server since last one minute.

Counters	Counter Descriptions
Video Get Media Capabilities Total	The total number of GetMediaCapabilities sent by Unity Connection to video server since the last restart of Unity Connection.
Video Get Media Capabilities In Last One Minute	The total number of GetMediaCapabilities sent by Unity Connection to video server since last one minute.
Video SignIn Total	The total number of SignIn request sent by Unity Connection to video server since the last restart of Unity Connection.
Video SignIn Total In Last One Minute	The total number of SignIn sent by Unity Connection to video server since last one minute.
KeyFrame Request sent Total	The total number of KeyFrame requests sent during video recording to EndPoint since the last restart of Cisco Unity Connection.
KeyFrame Request sent In Last One Minute	The total number of KeyFrame requests sent during video recording to EndPoint since the last restart of Cisco Unity Connection.
Video Record Successful Total	The total number of successful Video Recordings since the last restart of Cisco Unity Connection.
Video Sessions Failed Total	The total number of video sessions failed since the last restart of Cisco Unity Connection.
Video Session Failed In Last One Minute	The total number of video sessions failed in last one minute.
Media Sense Timeout Total	The total number of connection timeout errors while connecting to MediaSense server since the last restart of Cisco Unity Connection. This counter is applicable for the following events: • During a video call • At the time of sign in • During exchange of media capabilities with the MediaSense server.
Video Play Failed Total	The total number of video messages that are played as audio messages since the last restart of Cisco Unity Connection.

CUC Sessions: Voice

The CUC Sessions: Voice object provides information about voice sessions. The following table contains information on CUC Sessions: Voice counters.

Table 115: CUC Sessions: Voice

Counters	Counter Descriptions
Delay - Directory Search [ms]	The delay [in milliseconds] that a caller experienced when the caller attemp search through the directory. This counter measures the time between the e search criteria and the return results.
Delay - Opening Greeting [ms]	The delay [in milliseconds] that a caller experienced before any audio was This counter measures the time between the system receiving a call and the t begins streaming to the caller.
Delay - Subscriber Delete Message [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber exper when the subscriber attempted to delete a message. This counter measures between the last delete message prompt and the confirmation of the deletio
Delay - Subscriber Logon [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber experi to authentication.
Delay - Subscriber Message Count [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber exper during message counting in the subscriber message box.
Delay - Subscriber Message Header [ms]	The delay [in milliseconds] that a caller experienced while Cisco Unity Cor gathering message header information.
Failsafes Total	The total number of times that the failsafe conversation has been played.
G.711a Sessions Current	The current number of active G.711 (a-law) voice sessions.
G.711a Sessions Total	The total number of active G.711 (a-law) voice sessions since the last restar Unity Connection.
G.711u Sessions Current	The current number of active G.711 (u-law) voice sessions.
G.711u Sessions Total	The total number of active G.711 (u-law) voice sessions since the last restar Unity Connection.
G.722 Sessions Current	The current number of active G.722 voice sessions.
G.722 Sessions Total	The total number of active G.722 voice sessions since the last restart of Cis Connection.
G.729 Sessions Current	The current number of active G.729 voice sessions.
G.729 Sessions Total	The total number of active G.729 voice sessions since the last restart of Cis Connection.
iLBC Sessions Current	The current number of active iLBC voice sessions.
iLBC Sessions Total	The total number of active iLBC voice sessions since the last restart of Cis Connection.
Meeting search delay delay [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber experi to looking up meetings.

Counters	Counter Descriptions
Messages Deleted	The total number of voice messages that were deleted through the TUI Cisco Unity Connection was last restarted.
Messages Forwarded	The total number of voice messages that were forwarded through the T time Cisco Unity Connection was last restarted.
Messages Read	The total number of voice messages that were read through the TUI fro Cisco Unity Connection was last restarted.
Messages Replied	The total number of voice messages that received replies through the T time Cisco Unity Connection was last restarted.
Messages Sent	The total number of voice messages that were sent through the TUI fro Cisco Unity Connection was last restarted.
MRCP Define Grammar Delay [ms]	The delay [in milliseconds] between an MRCP define-grammar request an
MRCP Define Grammar Delay Average [ms]	The average delay [in milliseconds] between an MRCP define-gramma its response.
MRCP Define Grammar Delay Max [ms]	The maximum delay [in milliseconds] between an MRCP define-gramm its response.
MRCP Delay [ms]	The delay [in milliseconds] between an MRCP request and its response
MRCP Delay Average [ms]	The average delay [in milliseconds] between an MRCP request and its
MRCP Delay Max [ms]	The maximum delay [in milliseconds] between an MRCP request and i
OPUS Sessions Current	This displays the current number of active OPUS voice sessions.
OPUS Sessions Total	This displays the total number of OPUS voice sessions since the last re Unity Connection.
Sessions Current	The current number of all active voice sessions for any codec.
Sessions Total	The total number of voice sessions for any codec - G.711 mu-law and C the last restart of Cisco Unity Connection.
Subscriber Lookup Delay [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber ex to finding and loading a subscriber by DTMF ID.

CUC Sessions: VUI

The CUC Sessions: VUI object provides information about the voice user interface (VUI). The following table contains information on CUC Sessions: VUI counters.

Table 116: CUC Sessions: VUI

Counter	Counter Descriptions
Delay - Subscriber Message Access [ms]	The delay [in milliseconds] that a user when experienced when the user att access a message. This counter measures the time between the voice comm intending to listen to a message and the actual playback of the message.
Matches Total	The total number of matches in the VUI conversation.
Messages Read	The total number of messages that were read through the VUI from the time Unity Connection was last restarted.
No-matches Total	The total number of no-matches in the VUI conversation.
Session Duration Average/call [s]	The average duration [in seconds] of a VUI session as measured on a per-c
Session Duration Total [s]	The duration [in seconds] of all VUI sessions.
Sessions Current	The current number of active VUI sessions for any codec.
Sessions Total	The total number of VUI and voice sessions for any codec.

CUC Sessions: Web

The CUC Sessions: Web object provides information about the Cisco Personal Communications Assistant (Cisco PCA) and Cisco Unity Connection Administration sessions. The following table contains information on CUC Sessions: Web counters.

Table 117: CUC Sessions: Web

Counters	Counter Descriptions
CPCA Authentication Delay Max [s]	The maximum delay [in seconds] in authentication to a user Inbox or Assis
CPCA Failed Authentications Total	The number of failed authentications.
CPCA Pages Served Total	The total number of CPCA pages that the Cisco Unity Connection server s
CPCA Requests In Queue Current	The number of requests in CPCA queue waiting to be processed.
CPCA Server Busy Pages Total	The total number of server busy pages that the Cisco Unity Connection serve
CPCA Sessions Current	The current number of CPCA sessions.
CPCA Sessions Total	The total number of CPCA sessions.
CUCA Authentication Delay Max [s]	The maximum delay [in seconds] in authentication to the System Administrato
CUCA Response Time Max [ms]	The maximum time [in milliseconds] for the Tomcat server to respond to a request.

CUC Sessions: Web E-Mail Access

The CUC Sessions: Web E-mail Access object provides information about web e-mail access sessions (IMAP). The following table contains information about CUC Sessions: Web E-mail Access counters.

Table 118: CUC Sessions: Web E-Mail Access

Counters	Counter Descriptions
Messages Read - Total	The total number of e-mail messages that were read since the last restart c Connection.
Session Duration Average [ms]	The average duration [in milliseconds] of all e-mail sessions as measure basis.
Session Duration Total [ms]	The total duration [in milliseconds] of all e-mail sessions as measured c basis.
Sessions - Current	The number of active e-mail voice sessions.
Sessions - Total	The total number of e-mail voice sessions since the last restart of Cisco Connection.

CUC System Agent

The CUC System Agent object records the information about the periodic system tasks. The following table contains information about CUC System Agent counters.

Counters	Counter Descriptions
Message Related Files Shredded Total	The total number of messaging related files that have been shredded.
Message Related Files Shredded Failed	The total number of messaging related files that have failed to shred.
Total Number of Requests sent by HTTP[S]/CCI Link	The cumulative number of HTTP(S) requests sent by the Reader.
Total Number of successful response of HTTP[S]/CCI Requests	The cumulative number of HTTP(S) requests that were successfully processed by the Feeder.
Total Number of failure response of HTTP[S]/CCI Requests	The cumulative number of HTTP(S) requests that were not successfully processed by the Feeder.
Total Number of Directory Objects Successfully Processed	The cumulative number of Directory Objects that were successfully processed.
Directory Objects Processed Successfully In Last One Minute	Directory objects successfully processed per minute.

Counters	Counter Descriptions
Delete Request sent to Media Sense Total	The total number of delete requests sent to MediaSense server since the last restart of Unity Connection.
Media Sense Timeout While Delete Total	The total number of connection timeouts in response to the delete requests sent to MediaSense server since the last restart of Unity Connection.

CUC VMREST

The CUC VMREST object provides information about internal VMREST requests.

The following table contains information about VMREST counters.

Counters	Counter Description
Total VMREST active threads	To maintain Total Number of active VMREST threads.
Total VMREST Throttled Requests	To maintain Total Number of Throttled VMREST requests by Throttle Semaphore.
Total VMREST Throttled Requests in last hour	To maintain Total Number of Throttled VMREST requests by Throttle Semaphore in last hour.

CUC VMREST Container

The CUC VMREST Container object provides information about REST container operations for handling VMREST requests from external clients.

The following table contains information about VMREST Container counters.

Counters	Counter Description
Total VMREST CONTAINER active threads	To maintain Total Number of active VMREST threads for REST container.
Total VMREST CONTAINER throttled Requests	To maintain Total Number of Throttled VMREST requests by Throttle Semaphore for REST container.
Total VMREST CONTAINER throttled Requests in last hour	To maintain Total Number of Throttled VMREST requests by Throttle Semaphore in last hour for REST container.

System Alerts

AuditLogOverFlowDueToLogRotation

This alarm indicates that the audit log overflow occurred. An existing audit log file is overwritten resulting in overflow and eventual loss of audit data.

Default Configuration

Table 119: Default Configuration for the AuditLogOverFlowDueToLogRotation RTMT Alert

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

AuditLogOverflowDueToLPMPurge

This alarm indicates that overflow occurred due to purge by LPM clean-up logic. When the total disk space usage of log partition crosses the high water mark configured, the LPM tools clean-up logic deletes the oldest files from the log partition so that the new logs can be written.

Default Configuration

Table 120: Default Configuration for the AuditLogOverflowDueToLPMPurge RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

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

AuditLogsExceedsConfiguredThreshold

This alarm indicates the percentage of disk space configured for application audit logging exceeds the configured threshold. Audit logs files are overwritten sooner or later depends on the frequency of audit logging by the Unified Communications Manager applications.

Default Configuration

Table 121: Default Configuration for the AuditLogsExceedsConfiguredThreshold RTMT Alert

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

AuthenticationFailed

Authentication validates the user ID and password that are submitted during log in. An alarm gets raised when an invalid user ID and/or the password gets used.

Default Configuration

Table 122: Default Configuration for the AuthenticationFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Number of AuthenticationFailed events exceeds: 1 time in the last 1 minute
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CCMEncryptionErrorDetected

This alert occurs when the CCMEncryptionErrorDetected event is generated.

Default Configuration

Table 123: Default Configuration for the CCMEncryptionErrorDetected RTMT Alert

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

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

CiscoDRFFailure

This alert occurs when the DRF backup or restore process encounters errors.

Default Configuration

Table 124: Default Configuration for the CiscoDRFFailure 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: CiscoDRFFailure event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CiscoHAProxyServiceDown

The HAProxy Service Down alarm indicates when the incoming web traffic into Unified Communications Manager and IM and Presence Service is down.

The following table contains information about the CiscoHAProxyServiceDown counter.

Table 125: CiscoHAProxyServiceDown

Counters	Counter Description
Enable Alert	Selected
Severity	Warning
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: when HAProxy service do generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CoreDumpFileFound

This alert occurs when the CoreDumpFileFound event gets generated. This indicates that a core dump file exists in the system.

Default Configuration

Table 126: Default Configuration for the CoreDumpFileFound 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: CoreDumpFileFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Value	Default Configuration
Trace download Parameters	Not Selected
Enable Email	Selected
Trigger Alert Action	Default

CpuPegging

CPU usage gets monitored based on configured thresholds. If the usage goes above the configured threshold, this alert gets generated.

Default Configuration

Table 127: Default Configuration for the CpuPegging 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: 99%
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

CriticalServiceDown

The CriticalServiceDown alert gets generated when the service status equals down (not for other states).

Default Configuration

Table 128: Default Configuration for the CriticalServiceDown 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: Service status is DOWN
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 129: 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

Value	Default Configuration
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 130: Default Configuration for the DBReplicationFailure 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: 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

DBReplicationTableOutOfSync

Default Configuration

Table 131: Default Configuration for the DBReplicationTableOutOfSync 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 event with alarm number 888 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

HardwareFailure

This alert occurs when a hardware failure event (disk drive failure, power supply failure, and others) has occurred.

Default Configuration

Table 132: Default Configuration for the HardwareFailure 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: HardwareFailure event generated

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

LogFileSearchStringFound

This alert occurs when the LogFileSearchStringFound event gets generated. This indicates that the search string was found in the log file.

Default Configuration

Table 133: Default Configuration for the LogFileSearchStringFound 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: LogFileSearchStringFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LogPartitionHighWaterMarkExceeded

This alert occurs when the percentage of used disk space in the log partition exceeds the configured high water mark. When this alert gets generated, LPM deletes files in the log partition (down to low water mark) to avoid running out of disk space.

Note LPM may delete files that you want to keep. You should act immediately when you receive the LogPartitionLowWaterMarkExceeded alert.

Note In the case, when **logpartitionhighwatermarkexceeded** is set to a lower percentage and deletes the cdr/cmr files from the temporary folder then use **RTMT** to ensure that the alert parameter is set back to the default value of 95%.

Default Configuration

Table 134: Default Configuration for the LogPartitionHighWaterMarkExceeded 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: Log Partition Used Disk Space Exceeds High Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LogPartitionLowWaterMarkExceeded

This alert occurs when the LogPartitionLowWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the log partition has exceeded the configured low water mark.

Note Be aware that this alert is an early warning. The administrator should start freeing up disk space. Using RTMT/TLC, you can collect trace/log files and delete them from the server. The administrator should adjust the number of trace files that are kept to avoid hitting the low water mark again.

Default Configuration

Table 135: Default Configuration for the LogPartitionLowWaterMarkExceeded 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: Log Partition Used Disk Space Exceeds Low Water Mark (90%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowActivePartitionAvailableDiskSpace

This alert occurs when the percentage of available disk space on the active partition is lower than the configured value.

Default Configuration

Table 136: Default Configuration for the LowActivePartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers

Value	Default Configuration
Threshold	Trigger alert when following condition met: Active Partition available disk space below (4%) **Note** In customer environments, virtual machines configured with 80 GB disk space and where 91% or more space has been reserved for disk space/active partition, a 6% increase in utilization results in automatic trigger of the LowActivePartitionAvailableDiskSpace alert after the Unified Communications Manager upgrade. Here, the alert is triggered when the Active Partition available disk space is below (2%). You must log in to RTMT to fix this issue manually.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowAvailableVirtualMemory

RTMT monitors virtual memory usage. When memory runs low, a LowAvailableVirtualMemory alert is generated.

Default Configuration

Table 137: Default Configuration for the LowAvailableVirtualMemory 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: Available virtual memory below (15%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected

Value	Default Configuration
Trigger Alert Action	Default

LowInactivePartitionAvailableDiskSpace

This alert occurs when the percentage of available disk space of the inactive partition equals less than the configured value.

Default Configuration

Table 138: Default Configuration for the LowInactivePartitionAvailableDiskSpace 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: Inactive Partition available disk space below (4%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowSwapPartitionAvailableDiskSpace

This alert indicates that the available disk space on the swap partition is low.

Note The swap partition is part of virtual memory, so low available swap partition disk space means low virtual memory as well.

Default Configuration

Table 139: Default Configuration for the LowSwapPartitionAvailableDiskSpace 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: Swap Partition available disk space below (10%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ServerDown

This alert occurs when a remote node cannot be reached.

Note Unified Communications Manager and IM and Presence Service: The ServerDown alert is generated when the currently active AMC (primary AMC or the backup AMC, if the primary is not available) cannot reach another server in a cluster. This alert identifies network connectivity issues in addition to a server down condition.

Default Configuration

Table 140: Default Configuration for the ServerDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers

Value	Default Configuration
Threshold	Trigger alert when following condition met: ServerDown 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

SparePartitionHighWaterMarkExceeded

This alert occurs when the SparePartitionHighWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the spare partition exceeds the configured high water mark.

Default Configuration

Table 141: Default Configuration for the SparePartitionHighWaterMarkExceeded 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: Spare Partition Used Disk Space Exceeds High Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SparePartitionLowWaterMarkExceeded

This alert occurs when the SparePartitionLowWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the spare partition has exceeded the low water mark threshold.

Default Configuration

Table 142: Default Configuration for the SparePartitionLowWaterMarkExceeded 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: Spare Partition Used Disk Space Exceeds Low Water Mark (90%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SyslogSeverityMatchFound

This alert occurs when the SyslogSeverityMatchFound event gets generated. This indicates that a syslog message with the matching severity level exists.

Default Configuration

Table 143: Default Configuration for the SyslogSeverityMatchFound 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: SyslogSeverityMatchFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

Value	Default Configuration
Schedule	24 hours daily
Syslog Severity Parameters	Critical
Enable Email	Selected
Trigger Alert Action	Default

SyslogStringMatchFound

This alert occurs when the SyslogStringMatchFound event gets generated. The alert indicates that a syslog message with the matching search string exists.

Default Configuration

Table 144: Default Configuration for the SyslogStringMatchFound 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: SyslogStringMatchFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Syslog Alert Parameters	(Text box for search string)
Enable Email	Selected
Trigger Alert Action	Default

SystemVersionMismatched

This alert occurs when a mismatch in system version exists.

Default Configuration

Table 145: Default Configuration for the SystemVersionMismatched 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: SystemVersionMismatched 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

TCPRemoteSyslogDeliveryFailed

This alert occurs when delivery of alarms, audits, or syslog generate events to the configured remote syslog servers fails. The reason could be that the configured syslog server is down, or TCP is not configured on port 601, or there is a network failure.

Default Configuration

Table 146: Default Configuration for the TCPRemoteSyslogDeliveryFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TCPRemoteSyslogDeliveryFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

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

TLSRemoteSyslogDeliveryFailed

This alert occurs when delivery of alarms, audits, or syslog generate events to the configured remote syslog servers fails. The reason could be that the configured syslog server is down, or TLS over TCP is not configured on port 6514, or there is a network failure, or certificate of the remote syslog server is not uploaded to Unified Communications Manager Tomcat trust.

Default Configuration

Table 147: Default Configuration for the TLSRemoteSyslogDeliveryFailed RTMT Alert

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

TotalProcessesAndThreadsExceededThreshold

This alert occurs when the TotalProcessesAndThreadsExceededThreshold event gets generated. The alert indicates that the current total number of processes and threads exceeds the maximum number of tasks that are configured for the Cisco RIS Data Collector Service Parameter. This situation could indicate that a process is leaking or that a process has thread leaking.

Default Configuration

Table 148: Default Configuration for the TotalProcessesAndThreadsExceededThreshold 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: TotalProcessesAndThreadsExceededThreshold event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

Voice and Video Alerts

BeginThrottlingCallListBLFSubscriptions

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

Default Configuration

Table 149: 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

Value	Default Configuration
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

CallAttemptBlockedByPolicy

Default Configuration

Table 150: Default Configuration for the CallAttemptBlockedByPolicy 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: CallAttemptBlockedByPolicy event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
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.

If the administrator takes no action, high CPU pegging can lead to a Unified Communications Manager crash, especially in CallManager service. The CallProcessingNodeCpuPegging alert gives you time to work proactively to avoid a crash.

During CPU usage spikes, other alarms that may be issued in addition to the CallProcessingNodeCpuPegging alert include: CoreDumpFound, CriticalServiceDown, SDLLinkOutOfService, and NumberOfRegisteredPhonesDropped alarms.

Note Unified Communications Manager VMware installations can experience high CPU usage spikes while performing tasks such as DRF backups and Bulk Administration Tool exports. The processes that are commonly responsible for CPU usage spikes are gzip and DRFLocal.

If your system is generating CallProcessingNodeCpuPegging alarms, add an additional vCPU for the support of 7500 Unified Communications Manager users following the Open Virtualization Archives (OVA) template specifications for your system.

Default Configuration

Table 151: 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

CARIDSEngineCritical

Default Configuration

Table 152: Default Configuration for the CARIDSEngineCritical 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: CARIDSEngineCritical event generated.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CARIDSEngineFailure

Default Configuration

Table 153: Default Configuration for the CARIDSEngineFailure RTMT 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: CARIDSEngineFailure event generated.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

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

CARSchedulerJobFailed

Default Configuration

Table 154: Default Configuration for the CARSchedulerJobFailed RTMT 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: CARSchedulerJobFailed event generated.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
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 Unified Communications Manager node to a CDR repository node within the Unified Communications Manager cluster.

Default Configuration

Table 155: Default Configuration for the CDRAgentSendFileFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

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 156: 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

CDRFileDeliveryFailureContinues

This alert occurs when the CDRFileDeliveryFailureContinues event is generated. This indicates that FTP delivery of CDR files to the outside remote server failed after 3 or more attempts.

Default Configuration

Table 157: Default Configuration for the CDRFileDeliveryFailureContinues RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRFileDeliveryFailureContinues 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 158: 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

Value	Default Configuration
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 159: 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
Enable Email	Selected
Trigger Alert Action	Default

CiscoWLCSyncServiceDown

This alert occurs when the exceeded maximum number of devices(50000) in the Switches and Access points.

Default Configuration

Table 160: Default Configuration for the CiscoWLCSyncServiceDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CiscoWLCSyncServiceDown event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
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 161: 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

Value	Default Configuration
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

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 162: 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 163: 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

EMCCFailedInLocalCluster

Default Configuration

Table 164: Default Configuration for the EMCCFailedInLocalCluster RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers

Value	Default Configuration
Threshold	Trigger alert when following condition met: EMCCFailedInLocalCluster event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

EMCCFailedInRemoteCluster

Default Configuration

Table 165: Default Configuration for the EMCCFailedInRemoteCluster 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: EMCCFailedInRemoteCluster event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 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 166: 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
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ILSDuplicateURI

This alert occurs when the Unified Communications Manager identifies that it has learned duplicate URI entries through ILS during a call to the URI. Whenever there are duplicate entries for a URI(such as the URI user@example.com existing on two clusters), the call is routed to the cluster from which the URI that was first learned. Calls will not be routed to the other duplicate entries.

Default Configuration

Table 167: Default Configuration for the ILSDuplicateURI RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: ILSDuplicateURI event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

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

ILSHubClusterUnreachable

Default Configuration

Table 168: Default Configuration for the ILSHubClusterUnreachable RTMT 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: A connection to the remote ILS server could not be established.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ILSPeerLimitApproachingWarning

This alert occurs when the current peer count has reached 90% or more of the ILS network capacity.

Default Configuration

Table 169: Default Configuration for the ILSPeerLimitApproachingWarning RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

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

ILSPeerLimitExceeded

This alert occurs when the number of peers for this cluster in the ILS network is more than the limit set for ILSP_MSG_PEER_MAX. The system is allowed to add spokes, hubs, and imported catalogs continuously. However, only maximum number of peers are advertised to the ILS network.

Default Configuration

Table 170: Default Configuration for the ILSPeerLimitExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: The number of peers have exceeded the limit set for ILSP_MSG_PEER_MAX
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ILSPwdAuthenticationFailed

Default Configuration

Table 171: Default Configuration for the ILSPwdAuthenticationFailed RTMT 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: Password Authentication Failure with ILS at remote cluster.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ILSTLSAuthenticationFailed

Default Configuration

Table 172: Default Configuration for the ILSTLSAuthenticationFailed RTMT 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 ILS at remote cluster.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

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

IMEDistributedCacheInactive

This alarm gets generated when a 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 through the CLI.

Default Configuration

Table 173: 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 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 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 (Unified Communications Managers) on different Cisco IME services.

Default Configuration

Table 174: 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 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 175: Default Configuration for the IMEQualityAlert Alert

Value	Default Configuration
Enable Alert	Selected

Value	Default Configuration
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
Schedule	24 hours daily
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 (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 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 176: 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

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert every 60 minutes
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 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 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 177: 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

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within one minute
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InvalidCredentials

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

Default Configuration

Table 178: 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

LocationOutOfResource

This alert occurs when the number of LocationOutOfResource events exceeds the configure threshold during the configured time interval. This indicates that one or all of audio or video or immersive bandwidth for a location or link is used up.

Default Configuration

Table 179: Default Configuration for the LocationOutOfResource 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: LocationOutOfResource event generated 5 times within 60 seconds
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 Unified Communications Manager. The malicious call identification (MCID) feature gets invoked.

Default Configuration

Table 180: 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

Value	Default Configuration
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 181: 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
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 182: 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 183: Default Configuration for the NumberOfRegisteredDevicesExceeded 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: NumberOfRegisteredDevicesExceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Value	Default Configuration
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 184: 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 185: Default Configuration for the NumberOfRegisteredGatewaysIncreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

Value	Default Configuration
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 186: 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 187: 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 188: 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

RecordingCallSetupFail

Default Configuration

Table 189: Default Configuration for the RecordingCallSetupFail RTMT 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: RecordingCallSetupFail event(s) generated
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RecordingGatewayRegistrationRejected

Default Configuration

Table 190: Default Configuration for the RecordingGatewayRegistrationRejected RTMT 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: RecordingGatewayRegistrationRejected event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes

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

RecordingGatewayRegistrationTimeout

Default Configuration

Table 191: Default Configuration for the RecordingGatewayRegistratioNTimeout RTMT 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: RecordingGatewayRegistrationTimeout event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RecordingGatewaySessionFailed

Default Configuration

Table 192: Default Configuration for the RecordingGatewaySessionFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error

Value	Default Configuration
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: RecordingGatewaySessionFailed event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RecordingResourcesNotAvailable

Default Configuration

Table 193: Default Configuration for the RecordingResourcesNotAvailable 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: RecordingGatewayRegistrationTimeout event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RecordingSessionTerminatedUnexpectedly

Default Configuration

Table 194: Default Configuration for the RecordingSessionTerminatedUnexpectedly RTMT 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: RecordingCallSetupFail event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
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 195: 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

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

RTMTSessionsExceedsThreshold

Default Configuration

Table 196: Default Configuration for the RTMTSessionsExceedsThreshold RTMT 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: When number of ast session is more than 250.
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 Unified Communications Manager cannot communicate with the remote Unified Communications Manager. This event usually indicates network errors or a non-running remote Unified Communications Manager.

Default Configuration

Table 197: 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
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseAuthorizationExpiringSoon

This alert occurs when the Unified Communications Manager authorization with Cisco Smart Software Manager or Cisco Smart Software Manager satellite is going to expire soon.

Default Configuration

Table 198: Default Configuration for the SmartLicenseAuthorizationExpiringSoon RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseAuthorizationExpiringSoon event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

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

SmartLicenseCommunicationError

This alert occurs when Unified Communications Manager is unable to communicate successfully with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Default Configuration

Table 199: Default Configuration for the SmartLicenseCommunicationError RTMT Alert

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

SmartLicenseExportControlNotAllowed

This alert occurs when Unified Communications Manager is not registered with the Registration Token received from the Smart account or Virtual account that has Allow export-controlled functionality checked and is not licensed to operate in mixed-mode

Default Configuration

Table 200: Default Configuration for the SmartLicenseExportControlNotAllowed RTMT Alert

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

SmartLicenseInEval

This alert occurs when Unified Communications Manager is not registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite and is operating in Evaluation Mode that is soon going to expire.

Default Configuration

Table 201: Default Configuration for the SmartLicenseInEval RTMT Alert

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

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseInOverageAuthorizationExpired

This alert occurs when you do not renew the license authorization for Unified Communications Manager before the authorization expiry date and the license authorization has expired. It runs on the overage period that is soon going to expire.

Default Configuration

Table 202: Default Configuration for the SmartLicenseInOverage_AuthorizationExpired RTMT Alert

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

SmartLicenseInOverageOutOfCompliance

This alert occurs when Cisco Unified Communication Manager operates with insufficient number of licenses and the status is out of compliance. It runs on the overage period that is soon going to expire.

Default Configuration

Table 203: Default Configuration for the SmartLicenseInOverage_OutOfCompliance RTMT Alert

Value	Default Configuration
Enable Alert	Selected

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

SmartLicenseNoProvisionAuthorizationExpired

This alert occurs when the license authorization for Unified Communications Manager is not successful and the overage period has expired. You are not allowed to add, update, or delete any users or devices.

Default Configuration

Table 204: Default Configuration for the SmartLicenseNoProvision_AuthorizationExpired RTMT Alert

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

SmartLicenseNoProvisionEvalExpired

This alert occurs when the Cisco Smart Licensing evaluation period is expired for Unified Communications Manager. You are not allowed to add, update, or delete any users or devices.

Default Configuration

Table 205: Default Configuration for the SmartLicenseNoProvision_EvalExpired RTMT Alert

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

SmartLicenseNoProvisionOutOfCompliance

This alert occurs when Cisco Unified Communication Manager operates with insufficient number of licenses and the overage period has expired. You are not allowed to add, update, or delete any users or devices.

Default Configuration

Table 206: Default Configuration for the SmartLicenseNoProvision_OutOfCompliance RTMT Alert

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

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

SmartLicenseRegistrationExpired

This alert occurs when you do not renew the license registration for Unified Communications Manager before the registration expiry date and the license registration has expired. You are not allowed to add, update, or delete any users or devices.

Default Configuration

Table 207: Default Configuration for the SmartLicenseRegistrationExpired RTMT Alert

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

SmartLicenseRegistrationExpiringSoon

This alert occurs when the Unified Communications Manager registration with Cisco Smart Software Manager or Cisco Smart Software Manager satellite is going to expire soon.

Default Configuration

Table 208: Default Configuration for the SmartLicenseRegistrationExpiringSoon RTMT Alert

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

SmartLicenseRenewAuthFailed

This alert occurs when the Unified Communications Manager license authorization renewal fails.

Default Configuration

Table 209: Default Configuration for the SmartLicenseRenewAuthFailed RTMT Alert

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

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseRenewRegistrationFailed

This alert occurs when the Unified Communications Manager license registration renewal fails.

Default Configuration

Table 210: Default Configuration for the SmartLicenseRenewRegistrationFailed RTMT Alert

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

SmartLicense_Reservation_InEval

This alert occurs when Unified Communications Manager running in the Evaluation period is enabled for License Reservation and pending installation of reserved authorization code.

Default Configuration

Table 211: Default Configuration for the SmartLicense_Reservation_InEval RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning

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

SmartLicense_Reservation_NoProvision_EvalExpired

This alert occurs when the Unified Communications Manager license Evaluation period is expired and pending installation of Specified License Reservation or Permanent License Reservation authorization code.

Default Configuration

Table 212: Default Configuration for the SmartLicense_Reservation_NoProvision_EvalExpired RTMT Alert

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

SmartLicense_SLR_InOverage_NotAuthorized

This alert occurs when the Unified Communications Manager is running in Specified License Reservation mode and with insufficient number of licenses and the overage period is active.

Default Configuration

Table 213: Default Configuration for the SmartLicense_SLR_InOverage_NotAuthorized RTMT Alert

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

SmartLicense_SLR_NoProvision_NotAuthorized

This alert occurs when the Unified Communications Manager is running in Specified License Reservation mode and with insufficient number of licenses and the overage period has expired thereby moving into no provision state.

Default Configuration

Table 214: Default Configuration for the SmartLicense_SLR_NoProvision_NotAuthorized RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers

Value	Default Configuration
Threshold	Trigger alert when following condition met: **SmartLicense_SLR_NoProvision_NotAuthorized** event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicense_Reservation_ExportControlNotAllowed

This alert occurs when Unified Communication Manager has mixed-mode and License Reservation is enabled, and also when Unified Communication Manager is in Evaluation mode, Evaluation period expired, Registered-Specific License Reservation, and Registered-Permanent License Reservation states.

Default Configuration

Table 215: Default Configuration for the SmartLicense_Reservation_ExportControlNotAllowed RTMT Alert

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

SwitchesAndAccessPointReached75PercentCapacity

This alert occurs when the current record count for switches and access points has reached 75% of maximum capacity of 50000 records.

Default Configuration

Table 216: Default Configuration for the SwitchesAndAccessPointReached75PercentCapacity RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SwitchesAndAccessPointReached75PercentCapacity
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SwitchesAndAccessPointReached90PercentCapacity

This alert occurs when the current record count for switches and access points has reached 90% of maximum capacity of 50000 records.

Default Configuration

Table 217: Default Configuration for the SwitchesAndAccessPointReached90PercentCapacity RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SwitchesAndAccessPointReached90PercentCapacity
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

SwitchesAndAccessPointReached95PercentCapacity

This alert occurs when the current record count for switches and access points has reached 95% of maximum capacity of 50000 records.

Default Configuration

Table 218: Default Configuration for the SwitchesAndAccessPointReached95PercentCapacity RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SwitchesAndAccessPointReached95PercentCapacity
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 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 Unified Communications Manager 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 Unified Communications Manager servers and the Cisco IME server.

Default Configuration

Table 219: 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 Unified Communications Manager CTL.

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

Default Configuration

Table 220: 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

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

UserInputFailure

Default Configuration

Table 221: Default Configuration for the UserInputFailure 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: UserInputFailure event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IM and Presence Service Alerts

CTIGWModuleNotEnabled

Alert Description
This alert indicates that the Cisco CTI Gateway application is either not fully configured or enabled.
Unified RTMT Default Threshold
Not applicable.

Recommended Actions
Configure and enable the Cisco CTI Gateway application using the Unified Communications Manager IM and Presence CTI Gateway Settings page.

CTIGWProviderDown

Alert Description
This alert indicates that the CTI provider is down.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the connection to the configured Unified Communications Manager nodes and verify that the Cisco CTI Gateway application is enabled on the Cisco Unified CM IM and Presence Administration GUI CTI Settings page.

CTIGWProviderFailedtoOpen

Type
IM and Presence Service
Alert Description
This alert indicates that the CTI Provider failed to open due to a configuration error.
Unified RTMT Default Threshold
Not Applicable.
Recommended Actions
Verify the Unified Communications Manager addresses and application user credentials on the Administration GUI CTI Settings page.

CTIGWQBEFailedRequest

Alert Description
This alert indicates that the Cisco CTI Gateway application received a failed response to a request.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

CTIGWSystemError

Alert Description
This alert indicates Cisco CTI Gateway application system errors.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

CTIGWUserNotAuthorized

Alert Description
This alert indicates that the user failed to authorized due to wrong device or line DN.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Verify user device configuration and MOC settings.

CTIGWUserNotLicenced

Alert Description
This alert indicates that the user failed to authorize due to no license available.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the Cisco CTI Gateway application license and user configuration.

DuplicateDirectoryURI

Alert Description
This alert indicates that there are multiple users within the intercluster deployment that are assigned the same directory URI value when the Directory URI IM Address scheme is configured.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Take immediate action to correct the issue. Each user must be assigned a unique directory URI. Affected users may be homed on an intercluster peer.

DuplicateUserid

Alert Description
This alert indicates that there are duplicate user IDs assigned to one or more users on different clusters within the intercluster deployment.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Take immediate action to correct the issue. Each user must be assigned a unique user ID. The affected users may be homed on an intercluster peer.

EspConfigAgentFileWriteError

Alert Description
This alert indicates that the Cisco Config Agent service cannot write to the file system.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Using Unified RTMT, verify whether the disk space is low or exhausted. This alarm may indicate that the system is overloaded, which may require reassigning users to other nodes in the IM and Presence

Service cluster. You can reassign users to other nodes using the Topology page on the IM and Presence Service Administration GUI.

EspConfigAgentHighCPUUtilization

Alert Description
This alert indicates that CPU utilization has exceeded the configured threshold.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Unified RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

EspConfigAgentHighMemoryUtilization

Alert Description
This alert indicates that the virtual memory utilization has exceeded the configured threshold.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Unified RTMT to monitor memory utilization and reduce system load to improve performance if necessary.

EspConfigAgentLocalDBAccessError

Alert Description
This alert indicates that the Cisco Config Agent service failed to read or write to the local IM and Presence Service database.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Verify the system health using Cisco RTMT. Verify that the service A Cisco DB is running.

EspConfigAgentMemAllocError

Alert Description
This alert indicates that the Cisco Config Agent service cannot allocate memory.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Using Unified RTMT, verify if the system memory is low or exhausted. This alarm may indicate that the system is overloaded which may require reassigning users to other nodes in the IM and Presence Service cluster. You can reassign users to other nodes using the Topology page on the IM and Presence Service Administration GUI.

EspConfigAgentNetworkOutage

Alert Description
This alert indicates Cisco Config Agent network outage.

Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Verify system health and network connectivity using Cisco RTMT.

EspConfigAgentNetworkRestored

Alert Description
This alert indicates that Cisco Config Agent network is restored.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Verify system health and network connectivity using Cisco RTMT.

EspConfigAgentProxyDomainNotConfigured

Alert Description
This alert indicates that the Cisco Config Agent service is not configured. Cisco Config Agent service uses the proxy domain to properly generate ACLs. If not configured it could lead to routing failures.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Go to the Service Parameters drop-down menu on the IM and Presence Service publisher. Select the Cisco SIP Proxy service. Enter the IM and Presence Service domain into the Proxy Domain service parameter and save.

EspConfigAgentRemoteDBAccessError

Alert Description
This alert indicates that the Cisco Config Agent service cannot access a remote IM and Presence Service database.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Verify that the service A Cisco DB is running on the node specified in the alert. Sometimes these errors can be transient. In some cases the Config Agent may be accessing remote nodes that are not available for some reason. If that is the case, then this error is expected. This result would happen in a user reassignment to a node that is not installed or available.

EspConfigAgentSharedMemoryStaticRouteError

Alert Description
This alert indicates that the Cisco Config Agent service failed to access static routes in shared memory. This may indicate that the system is out of memory.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Using Cisco RTMT, verify if the system shared memory is low or exhausted. This alarm may indicate the system is overloaded which may require reassigning users to other nodes in the IM and Presence

Service cluster. You can reassign users to other nodes using the Topology page on the Administration GUI.

ESPConfigError

Alert Description
This alert indicates Cisco SIP Proxy service configuration file error.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Verify that the Cisco Config Agent service is running. This service is responsible for writing the proxy configuration file.

ESPConfigNotFound

Alert Description
This alert indicates that Cisco SIP Proxy service configuration file is not found.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Verify that the configuration files `/usr/local/sip/conf/sipd.conf` and `/usr/local/sip/conf/dynamic.sipd.conf` exist on the IM and Presence server.

ESPCreateLockFailed

Alert Description
This alert indicates that lock file has not been created.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPLoginError

Alert Description
This alert indicates that an error occurred while communicating with the login datastore.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPMallocFailure

Alert Description
This alert indicates that memory allocation has failed. This may indicate a low or no memory issue with the server.
Unified RTMT Default Threshold
Not applicable.

Recommended Actions
Use Unified RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPNAPTRInvalidRecord

Alert Description
This alert indicates that NAPTR record format error.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPPassedParamInvalid

Alert Description
This alert indicates that invalid parameters were specified. This could be because the parameters were NULL.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Unified RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPRegistryError

Alert Description
This alert indicates that it is not possible to add registration to the SIP Registry because a resource limit was exceeded.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPRoutingError

Alert Description
This alert indicates SIP Route Interface resource limit exceeded error.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPSharedMemAllocFailed

Alert Description
This alert indicates that the Cisco SIP Proxy service failed to allocate shared memory segments while trying to initialize tables.
Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Use Unified RTMT to check system shared memory, check the Cisco SIP Proxy service trace log file for any detailed error messages and contact Cisco TAC for assistance.

ESPSharedMemCreateFailed

Alert Description
This alert indicates that the Cisco SIP Proxy service failed to create shared memory segments while trying to initialize tables.
Unified RTMT Default Threshold
Not Applicable
Recommended Actions
Use Unified RTMT to check system shared memory, check the Cisco SIP Proxy service trace log file for any detailed error messages, and contact Cisco TAC for assistance.

ESPSharedMemSetPermFailed

Alert Description
This alert indicates that the Cisco SIP Proxy service failed to set permissions on shared memory segments while trying to initialize tables.
Unified RTMT Default Threshold
Not Applicable
Recommended Actions
Use Unified RTMT to check system shared memory, check the Cisco SIP Proxy service trace log file for any detailed error messages, and contact Cisco TAC for assistance.

ESPSocketError

Alert Description
This alert indicates network socket errors that could be caused by binding errors such as get socket address failures.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPStatsLogFileOpenFailed

Alert Description
This alert indicates that the Cisco SIP Proxy service stats log file has failed to open.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPStopped

Alert Description
This alert indicates that the Cisco SIP Proxy service child process has stopped.
Unified RTMT Default Threshold
Not Applicable
Recommended Actions
If the administrator has not manually stopped the Proxy service, this may indicate a problem. Use Unified RTMT to check for any related alarms and contact Cisco TAC for assistance.

ESPVirtualProxyError

Alert Description
This alert indicates Virtual_Proxy_Domain related error.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPWrongHostName

Alert Description
This alert indicates an invalid IP address or an unresolvable hostname.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPWrongIPAddress

Alert Description
This alert indicates that an invalid IP address has been provided.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ICSACertificateCAConflict

Alert Description
This alert indicates that the Cisco Intercluster Sync Agent service detected a CA certificate conflict.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
A conflicting CA certificate was detected on Unified Communications Manager when auditing certificates. Stop the Cisco Intercluster Sync Agent on all IM and Presence nodes in the cluster. Delete the conflicting certificate on all IM and Presence and Unified Communications Manager nodes and re-upload the valid certificate to each node. Start the Cisco Intercluster Sync Agent.

ICSACertificateCASignedTrustCertFound

Alert Description
This alert indicates that the Cisco Intercluster Sync Agent service has detected a signed CA trust certificate.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Allow only unsigned CA trust certificates.

ICSACertificateFingerPrintMisMatch

Alert Description
This alert indicates that the Cisco Intercluster Sync Agent service detected a fingerprint mismatch on the certificate being processed.
Unified RTMT Default Threshold
Not Applicable
Recommended Actions
Use the IM and Presence Service OS Administration GUI to compare the certificates that are loaded on this server with the certificates on the source server. You might need to delete the problem certificates and reload them.

ICSACertificateValidationFailure

Alert Description
This alert indicates that the Cisco Intercluster Sync Agent service detected a validation error on the certificate being processed.
Unified RTMT Default Threshold
Not Applicable
Recommended Actions
Use the IM and Presence OS Administration GUI to compare the certificates that are loaded on this server with the certificates on the source server. You might need to delete the problem certificates and reload them.

InterclusterSyncAgentAXLConnectionFailed

Alert Description
This alert indicates that the Cisco Intercluster Sync Agent service failed authentication to the remote IM and Presence Service cluster and therefore cannot connect.
Unified RTMT Default Threshold
Not Applicable.
Recommended Actions
Verify that the AXL credentials are correct and whether the Cisco AXL Web service is running on the remote IM and Presence Service cluster.

InterclusterSyncAgentPeerDuplicate

Alert Description

This alert indicates that the Cisco Intercluster Sync Agent service failed to sync user location data from a remote peer. The remote peer is from an IM and Presence Service cluster that already has a peer in the local cluster.

Unified RTMT Default Threshold

Not Applicable.

Recommended Actions

Verify that the hostname of the remote peer is not a secondary node from the identified existing peer. If the new peer is a secondary node, then remove this peer from the IM and Presence Service Administration GUI Inter-cluster details page. You can also run the System Troubleshooter for more details.

InvalidDirectoryURI

Alert Description

This alert indicates that one or more users within the deployment are assigned an empty or invalid directory URI value when the Directory URI IM Address scheme is configured.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Take immediate action to correct the issue. Affected users may be homed on an intercluster peer.

JSMSessionsExceedsThreshold

This alert indicates when the client registrations get out of hand and exceeds the number of sessions created on the node.

The following table contains information about the JSMSessionsExceedsThreshold counter.

Table 222: JSMSessionsExceedsThreshold

Counters	Counter Description
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: when JsmTotalSessionsThresho exceeds the threshold
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected

Counters	Counter Description
Trigger Alert Action	Default

LegacyCUPCLogin

Alert Description
This alert indicates that a legacy Cisco Unified Personal Communicator client has attempted to login to the Cisco Client Profile Agent service.

Unified RTMT Default Threshold
Not applicable.

Recommended Actions
Upgrade the legacy Cisco Unified Personal Communicator client as it is currently not supported.

NotInCucmServerListError

Alert Description
This alert indicates that the Cisco Sync Agent failed to start because the IM and Presence node is not in the server list on the Unified Communications Manager publisher.

Unified RTMT Default Threshold
Not applicable.

Recommended Actions
Add the IM and Presence node to the server list on the Unified Communications Manager server and start the Cisco Sync Agent service.

PEAutoRecoveryFailed

Alert Description
This alert indicates that an error occurred during the startup sequence of the Cisco Presence Engine service.

Unified RTMT Default Threshold
Not applicable.

Recommended Actions
This error may indicate a possible configuration issue. Correct the problem identified in the failure message.

PEDatabaseError

Alert Description
This alert indicates that the Cisco Presence Engine service encountered an error while retrieving information from the database. This may indicate a problem with the Cisco DB service.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Verify that the Cisco DB service is running. Use Unified RTMT to check the Cisco Presence Engine service logs for errors. Consult Cisco TAC for guidance.

PEIDSQueryError

Alert Description

This alert indicates that the Cisco Presence Engine service has detected an error while querying the IM and Presence Service database.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Restart the Cisco Presence Engine service when convenient. See the associated error message and log files and consult Cisco TAC if the problem persists.

PEIDSSubscribeError

Alert Description

This alert indicates that the Cisco Presence Engine service was unable to subscribe for IM and Presence Service database change notifications.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Restart the Cisco Presence Engine service when convenient. See the associated error message and log files and consult Cisco TAC if the problem persists.

PEIDStoIMDBDatabaseSyncError

Alert Description

This alert indicates that synchronization between the IM and Presence database and the Cisco Presence Engine and a database service has failed (Cisco Login Datastore, Cisco Route Datastore, Cisco Presence Datastore, and Cisco SIP Registration Datastore).

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Restart the Cisco Presence Engine service when convenient. See associated error message and log files and consult Cisco TAC if the problem persists.

PELoadHighWaterMark

Alert Description

This alert indicates that the Cisco Presence Engine service has exceeded CPU utilization threshold.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Inspect the number of active subscription counters using Cisco RTMT: ActiveSubscriptions, ActiveViews, SubscriptionActiveReceivedFromForeign, and SubscriptionActiveSentForeign. If this condition persists, you may consider moving users to a different IM and Presence Service node in the cluster.

PEMemoryHighCondition

Alert Description
This alert indicates that the Cisco Presence Engine service has hit a high memory threshold.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the number of active subscription counters: ActiveSubscriptions, ActiveViews, SubscriptionActiveReceivedFromForeign, and SubscriptionActiveSentForeign using Unified RTMT. If this condition persists, offload some users to a different IM and Presence node in the cluster.

PEPeerNodeFailure

Alert Description
This alert indicates that Cisco Presence Engine service on the peer node of a subcluster has failed.
Unified RTMT Default Threshold
Not Applicable
Recommended Actions
Use Cisco Unified Serviceability to verify that the Cisco Presence Engine service is running. Consult Cisco TAC for further assistance.

PESipSocketBindFailure

Alert Description
This alert indicates that the Cisco Presence Engine service cannot connect to the indicated configured interface. No SIP traffic can be processed on this interface.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Verify that the Cisco Presence Engine service listen interface is configured correctly on the IM and Presence Service Administration GUI Application Listener page. Verify that no other process is listening on the same port using netstat.

PEStateDisabled

Alert Description
This alert indicates that the Cisco Presence Engine service is inoperable and cannot process traffic.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the log files and monitor the Cisco Presence Engine service with Unified RTMT.

PEStateLocked

Alert Description
This alert indicates that the Cisco Presence Engine service is administratively prohibited from processing traffic.
Unified RTMT Default Threshold
Not applicable.

Recommended Actions
This alert is only for notification purpose. No action is required.

PEWebDAVInitializationFailure

Alert Description
This alert indicates that the Cisco Presence Engine service has failed to initialize the WebDAV library.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Restart the Cisco Presence Engine service.

PWSAboveCPULimit

Alert Description
This alert indicates that the Presence Web Service module running in the Cisco SIP Proxy service has detected that the CPU utilization has exceeded the configured threshold. During this time, new requests are blocked until the CPU utilization drops below the configured threshold.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Using Unified RTMT, inspect the Cisco SIP Proxy service logs for more details.

PWSAboveSipSubscriptionLimit

Alert Description
This alert indicates that the Presence Web Service running in the Cisco SIP Proxy service has detected that the subscription count has exceeded the configured limit. During this time the Presence Web Service will block new incoming SIP subscriptions until the subscription count drops below the configured limit.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Using Cisco RTMT, inspect the Cisco SIP Proxy service logs for more details.

PWSRequestLimitReached

Alert Description
This alert indicates that the Cisco SIP Proxy service request per second limit has been reached.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
You may need to throttle back the incoming request rate.

PWSSCBFindFailed

Alert Description
This alert indicates that a call to find_scb() returned NULL which indicates the SCB lookup failed.

Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

PWSSCBInitFailed

Alert Description
This alert indicates that SCB init has failed.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Restart the Cisco SIP Proxy service.

ReplicationDefaultIMDomainChangeFailure

Alert Description
This alert occurs when a local default IM domain change fails.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Rerun the local default IM domain change procedure from the Advanced Presence Setting page.

ReplicationIMAddressSchemeChangeFailure

Alert Description
This alert occurs when an IM Address Scheme change fails.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Rerun the IM Address Scheme change procedure from the Advanced Presence Settings page.

SRMFailover

Type
IM and Presence Service
Alert Description
This alert indicates that the Server Recovery Manager is performing an automatic failover.
Unified RTMT Default Threshold
Not Applicable
Recommended Actions
Verify that the failed node is up and that critical services are running.

SRMFailed

Alert Description
This alert indicates that the Server Recovery Manager is in the Failed state.

Unified RTMT Default Threshold
Not Applicable
Recommended Actions
When it is convenient restart the Server Recovery Manager.

SyncAgentAXLConnectionFailed

Alert Description
This alert occurs when the Cisco Sync Agent service failed authentication.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Please verify that the AXL credentials are correct and whether the Cisco AXL Web service is activated and running on the remote Unified Communications Manager publisher.

UASCBFindFailed

Alert Description
This alert indicates that a call to find_scb() returned NULL which indicates the SCB lookup failed.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

UASCBGetFailed

Alert Description
This alert indicates that a call to tcbtable_acquire_tcb() returned NULL which indicates a SCB get/create failure.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

XcpCmComponentConnectError

Alert Description
This alert indicates that the Cisco XCP Connection Manager is shutting down because it failed to connect to the Cisco XCP Router.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the Cisco XCP Connection Manager log file for more details.

XcpCmConnectionsPerIpLimit

Alert Description
This alert indicates a limit on the maximum number of simultaneous XMPP client connections to the XCP Connection Manager emanating from the same IP address.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the Cisco XCP Connection Manager log file for more details.

XcpCmPauseSockets

Alert Description
This alert indicates that the outstanding XCP internal packet or database requests have reached configured limit. Client connections will be paused until pending requests have dropped back below threshold. Users will experience lag until issue is resolved. Users may be disconnected if configured timeout is reached before resolution.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the XCP Router log file for more details. Monitor client disconnecting due to timeout from the XCP Connection Managers.

XcpCmStartupError

Alert Description
This alert indicates that the XCP Connection Manager service failed to startup.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the CM log file for more details.

XcpCmXmppdError

Alert Description
This alert indicates that the XCP Connection Manager (CM) service has errors in the XMPP interface.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the CM log file for more details.

XCPConfigMgrConfigurationFailure

Alert Description

This alert indicates that the Cisco XCP Config Manager failed to successfully update XCP configuration.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions

See the Cisco XCP Config Manager logs for the root cause. Contact Cisco TAC for assistance.

XCPConfigMgrHostNameResolutionFailed

Alert Description

This alert indicates that the Cisco XCP Config Manager could not resolve a DNS name to allow Cisco XCP Routers to connect to that node.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Verify DNS resolvability of all hostnames and FQDNs in both local and remote clusters. Restart the Cisco XCP Config Manager and then restart the Cisco XCP Router after DNS is resolvable.

XCPConfigMgrJabberRestartRequired

Alert Description

This alert indicates that the Cisco XCP Config Manager has regenerated XCP XML files after system halt due to buffer size. The Cisco XCP Router must now be restarted to apply changes.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

When it is convenient to do so, restart the Cisco XCP Router.

XCPConfigMgrR2RPasswordEncryptionFailed

Alert Description

This alert indicates that the Cisco XCP Config Manager was unable to encrypt the password that is associated with an Inter-cluster Router-to-Router configuration.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

When it is convenient to do so, restart the Cisco XCP Config Manager and then restart the Cisco XCP Router.

XCPConfigMgrR2RRequestTimedOut

Alert Description

This alert indicates that Cisco XCP Config Manager sent an R2R configuration request to the XCP Router, but the XCP Router did not acknowledge the request in the time allowed.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Restart the Cisco XCP Config Manager and then restart the XCP Router.

XcpDBConnectError

Alert Description

Cisco XCP data access layer was unable to connect to the DB. This may indicate that the local or external database is down or the network connectivity to the external database is lost.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the System Troubleshooter for more information. Also check that the external database is running healthy and if there is any problem with the network connectivity to the external database server.

XcpMdnsStartError

Alert Description

This alert indicates that the XCP Router failed to startup the Multicast Domain Name Service (MDNS). This can cause connectivity failures to other routers in the cluster.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the XCP Router log file for more details.

XcpMessArchDBConnectError

Alert Description

This alert occurs when the Cisco XCP data access layer was unable to connect to the dB.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Please check the System Troubleshooter for more information. Also check that the external database is running healthy and if there is any problem with the network connectivity to the external database server.

XcpMessArchDBFullError

Alert Description

This alert occurs when the Cisco XCP data access layer was unable to insert data into the dB due to insufficient disk space or tablespace.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Please free up the disk space or tablespace on the external dB.

XcpMFTDBConnectError

Alert Description

This alert indicates that the Cisco XCP data access layer was unable to connect to the external database.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Check the System Troubleshooter for more information. Also check that the external database is running healthy and if there is a problem with the network connectivity to the external database server.

XcpMFTDBFullError

Alert Description

This alert occurs when the Cisco XCP data access layer was unable to insert data into the dB due to insufficient disk space or tablespace.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Please free up the disk space or tablespace on the dB.

XcpMFTExtFsFreeSpaceWarn

Alert Description

This alert indicates that the Cisco XCP File Transfer Manager has detected that the available disk space on the external file server is low.

Unified RTMT Default Threshold

Less than 10% of the file server disk space remains.

Recommended Actions

The alert is cleared by increasing disk space to greater than 15%. Free up space on the external file server by deleting unwanted files from the partition used for file transfers.

XcpMFTExtFsMountError

Alert Description

This alert indicates that the Cisco XCP File Transfer Manager has lost its connection to the external file server.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Check the External File Server Troubleshooter for more information. Also check that the external file server is running correctly or if there is a problem with the network connectivity to the external file server.

XcpSIPFedCmComponentConnectError

Alert Description

This alert indicates that the Cisco XCP SIP Federation Connection Manager is shutting down as it failed to connect to the Cisco XCP Router.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions
Check the Cisco XCP SIP Federation Connection Manager log file for more details.

XcpSIPFedCmPauseSockets

Alert Description
This alert occurs when the XCP Router has directed the XCP SIP Federation Connection Manager (CM) to pause listening on its socket due to load on the system.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Please check the XCP Router log file for more details. Watch for the client disconnecting due to timeout from the XCP Connection Managers.

XcpSIPFedCmStartupError

Alert Description
This alert indicates that the Cisco XCP SIP Federation Connection Manager service has failed to start.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the Cisco XCP SIP Federation Connection Manager log file for more details.

XcpSIPGWStackResourceError

Alert Description

This alert indicates that the maximum supported concurrent SIP Federation subscriptions or SIP Federation IM sessions has been reached, and the Cisco XCP SIP Federation Connection Manager does not have the resources that are required to handle any addition subscriptions or IM sessions.

Unified RTMT Default Threshold
Not Applicable
Recommended Actions

Increase the Pre-allocated SIP stack memory Service Parameter for the Cisco XCP SIP Federation Connection Manager. Note: If you are changing this setting, make sure that you have the memory available. If you do not have enough memory, you may have reached the limit of your hardware capability.

XcpThirdPartyComplianceConnectError

Alert Description
This alert indicates that Cisco XCP Router is unable to connect to the Third Party Compliance Server. This may be because of a network problem or a Third Party Compliance Server configuration or licensing problem.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
This is a serious error that breaks IM on the IM and Presence Service. Check network connection to and configuration(including licensing) on Third Party Compliance Server. To restore IM services set the

Compliance Settings option in the Administration GUI to Not Configured until the connection failure cause is identified.

XcpTxtConfComponentConfigError

Alert Description
This alert occurs when the XCP component detected a bad configuration.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Please check the component log file for more details.

XcpTxtConfDBConnectError

Alert Description
This alert indicates that the Cisco XCP Text Conferencing data access layer was unable to connect to the external database.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the system troubleshooter for more information. Also check if the external database is running properly and if there is any problem with the network connectivity to the external database server.

XcpTxtConfDBFullError

Alert Description
This alert occurs when the Cisco XCP data access layer was unable to insert data into the dB due to insufficient disk space or tablespace.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Please free up the disk space or tablespace on the dB.

XcpTxtConfDbQueueSizeLimitError

Alert Description
This alert occurs when the number of dBrequests has reached the maximum limit specified by the configuration.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the state of the external database server and check that it is accessible over the network. Then restart the Cisco XCP Text Conference Manager on CUP.

XcpTxtConfGearError

Alert Description
This alert indicates that the XCP Text Conference Manager (TC) Service has failed to load a configured component. This can prevent the service to start or behave as expected.

Unified RTMT Default Threshold
Not applicable.

Recommended Actions
Check the XCP Text Conference log file for more details.

XcpTxtConfTCMessagesMsgIdError

This alert occurs when the XCP component detected an error message.

The following table contains information about the XcpTxtConfTCMessagesMsgIdError counter.

Table 223: XcpTxtConfTCMessagesMsgIdError

Counters	Counter Description
Enable Alert	Selected
Severity	Error
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: when Invalid state of table in the external database event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

XcpWebCmComponentConnectError

Alert Description
This alert indicates that the Cisco XCP Web Connection Manager is shutting down as it failed to connect to the Cisco XCP Router.

Unified RTMT Default Threshold
Not applicable.

Recommended Actions
Check the Cisco XCP Web Connection Manager log file for more details.

XcpWebCmHttpdError

Alert Description
This alert indicates that the Cisco XCP Web Connection Manager service has errors in the HTTP interface.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the Cisco XCP Web Connection Manager log file for more details.

XcpWebCmPauseSockets

Alert Description
This alert occurs when the XCP Router has directed the XCP Web Connection Manager (CM) to pause listening on its socket due to load on the system.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Please check the XCP Router log file for more details. Watch for the client disconnecting due to timeout from the XCP Connection Managers.

XcpWebCmStartupError

Alert Description
This alert indicates that the Cisco XCP Web Connection Manager service has failed to start.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the Cisco XCP Web Connection Manager log file for more details.

XcpXMPPFedCmComponentConnectError

Alert Description
This alert indicates that the Cisco XCP XMPP Federation Connection Manager is shutting down because it failed to connect to the Cisco XCP Router.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Check the Cisco XCP XMPP Federation Connection Manager log file for more details.

XcpXMPPFedCmPauseSockets

Alert Description
This alert occurs when the XCP Router has directed the XCP XMPP Federation Connection Manager (CM) to pause listening on its socket due to load on the system.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Please check the XCP Router log file for more details. Watch for the client disconnecting due to timeout from the XCP Connection Managers.

XcpXMPPFedCmStartupError

Alert Description
This alert occurs when the XCP XMPP Federation Connection Manager service failed to startup.
Unified RTMT Default Threshold
Not applicable.
Recommended Actions
Please check the CM log file for more details.

Intercompany Media Engine Alerts

BannedFromNetwork

This alert indicates that network administrators have banned this Cisco IME server from the network (IME distributed cache ring), making this Cisco IME service fully or partly inoperative. Network administrators rarely ban servers but do so if they detect that the server is being used to launch malicious attacks into the network. If you receive this alert in error, contact TAC immediately.

Default Configuration

Table 224: Default Configuration for the BannedFromNetwork 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: Cisco IME service banned from network
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEDistributedCacheCertificateExpiring

This alert indicates the number of days that remain until the certificate that is used for the IME distributed cache expires. You must replace the certificate prior to expiration.

Default Configuration

Table 225: Default Configuration for the IMEDistributedCacheCertificateExpiring 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: Cisco IME distributed cache certificate about to expire. 14 days.
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within 1440 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEDistributedCacheFailure

This alert indicates the health of the IME distributed cache. A value of zero (red) means that the IME distributed cache is suffering from a significant problem such as one of the following conditions:

- The Cisco IME cannot resolve issues after the network was partitioned. In this case, validation attempts may fail.
- The Cisco IME service is not connected to the network at all and is unable to reach the bootstrap servers.

A value of one (yellow) indicates that the Cisco IME network is experiencing minor issues, such as connectivity between bootstrap servers or other Cisco IME network issues. Check for any alarms that may indicate why this counter is 1. A value of two indicates that IME distributed cache is functioning normally and the system is considered healthy.

Default Configuration

Table 226: Default Configuration for the IMEDistributedCacheFailure Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert

Value	Default Configuration
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: IME distributed cache failure in states 1: network experience minor issues 0: network in trouble
Duration	Trigger alert immediately
Frequency	Trigger 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMESdlLinkOutOfService

This alert indicates that the Cisco IME service has lost communication with Cisco IME Config Manager services, such as the Cisco AMC Service or the Cisco CallManager Service.

This alert usually indicates that one of these services has gone down (either intentionally, for maintenance; or unintentionally, due to a service failure or connectivity failure).

Default Configuration

Table 227: Default Configuration for the IMESdlLinkOutOfService 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: SDLLinkOOS event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

InvalidCertificate

This alert indicates that the administrator enabled the IME distributed cache on the Cisco IME server but omitted the configuration of a valid certificate or configured an incorrect certificate.

Default Configuration

Table 228: Default Configuration for the InvalidCertificate 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: Invalid certificate configured
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InvalidCredentials

The alert indicates that the Unified Communications Manager cannot connect to the Cisco IME server, because the username and password that are configured on 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 username and password that are configured match those configured in Unified Communications Manager.

Default Configuration

Table 229: Default Configuration for the InvalidCredentials 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: Invalid or mismatched credentials.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

MessageOfTheDay

The Cisco IME service generates this alert when the administrators of the Cisco IME network have a message for you.

Default Configuration

Table 230: Default Configuration for the MessageOfTheDay Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Notice
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Message from network administrators
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 1440 minutes

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

SWUpdateRequired

The Cisco IME server generates this alert when a new version of the Cisco IME server software is required. This alert repeats until you perform the upgrade. To obtain more information about the software update, go to the Cisco website. You should install critical updates within days of receiving this alert.

These upgrades address security vulnerabilities or key functional outages. In some cases, if you do not apply a critical upgrade immediately, the Cisco IME server may become unable to connect to the network.

Default Configuration

Table 231: Default Configuration for the SWUpdateRequired 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: Software update required
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TicketPasswordChanged

The Cisco IME server generates this alert when the administrator changes the password that is used to generate the validation tickets.

Verify that an authorized administrator changed the password. Unauthorized changes may indicate compromise to the administrative interfaces on the Cisco IME service. If you determine that unauthorized changes have been made, change the administrative passwords on the Cisco IME server immediately to prevent further

unauthorized access. To change the administrative password, type **set password admin** in the Cisco IME server CLI.

Default Configuration

Table 232: Default Configuration for the TicketPasswordChanged Alert

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

ValidationsPendingExceeded

This alert indicates the number of pending validations on the Cisco IME server. This number provides an indicator of the backlog of work on the Cisco IME server.

Default Configuration

Table 233: Default Configuration for the ValidationsPendingExceeded 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 IME pending validations exceeded 100

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

Cisco Unity Connection Alerts

NoConnectionToPeer

(Cisco Unity Connection cluster configuration) This alert is generated when the servers of a Cisco Unity Connection cluster cannot communicate with each other (for example, when the network connection is lost).

Default Configuration

Table 234: Default Configuration for the NoConnectionToPeer RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: NoConnectionToPeer event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

AutoFailoverSucceeded

(Cisco Unity Connection cluster configuration) This alert is generated in the following conditions:

- When the server with the Secondary status automatically changes its status to Primary (for example, when a critical failure occurs on the server with the Primary status) and assumes responsibility for handling the voice messaging functions and database for the cluster. This alert signals that the following events occurred:
  - The server that originally had the Primary status experienced a serious failure.
  - The server that originally had the Secondary status now has the Primary status and is handling all calls successfully.
- When the server that stopped functioning (described above) is brought back online and the server status automatically changes so that both servers resume sharing responsibility for handling the voice messaging functions and replication.

Default Configuration

Table 235: Default Configuration for the AutoFailoverSucceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: AutoFailoverSucceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

AutoFailoverFailed

(Cisco Unity Connection cluster configuration) This alert is generated in the following conditions:

- When the server with the Secondary status attempts to automatically change its status to Primary (for example, when a critical failure occurs on the server with the Primary status), but the automatic server status change fails so that the server with the Secondary status keeps the Secondary status.
- When a server that has stopped functioning (for example, a critical failure occurred) is not brought back online. Only one server in the cluster is functioning.

Default Configuration

Table 236: Default Configuration for the AutoFailoverFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: AutoFailoverFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

AutoFailbackSucceeded

(Cisco Unity Connection cluster configuration) This alert is generated when the problem that caused the server with the Primary status to stop functioning (causing the server with the Secondary status to change its status to Primary) is resolved and both servers are again online. Then, the servers automatically change status so that the server that had stopped functioning has the Primary status and the other server has the Secondary status.

Default Configuration

Table 237: Default Configuration for the AutoFailbackSucceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: AutoFailbackSucceeded event generated

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

AutoFailbackFailed

(Cisco Unity Connection cluster configuration): This alert occurs when the publisher node is not online and the server with the Primary status fails to automatically change status.

Default Configuration

Table 238: Default Configuration for the AutoFailbackFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: AutoFailbackFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SbrFailed (Split Brain Resolution Failed)

When a Cisco Unity Connection cluster is configured, if two servers cannot communicate with each other, they will both have the Primary status at the same time (a “split brain” condition), handle voice messaging functions, save messages to their own message stores, but not perform any replication. Users can retrieve their messages, but only one server knows that these messages have been retrieved.

When both servers are able to communicate with each other, they resolve this split brain condition by determining the correct contents and state of each user mailbox:

- Whether new messages that have been received.
- Whether MWIs for new messages have already been sent.
- Which messages have been listened to.
- Which messages have been deleted.

If the resolution of the split brain condition fails, this alert occurs.

Default Configuration

Table 239: Default Configuration for the SbrFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational
Threshold	Trigger alert when following condition met: SbrFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DiskConsumptionCloseToCapacityThreshold

This alert is generated when the hard disk usage on the Cisco Unity Connection server reaches ten percent below the percentage limit that the **System Settings** > **Advanced** > **Disk Capacity** window in Cisco Unity Connection Administration specifies. For example, with a capacity threshold limit of 95 percent, the alert gets triggered when usage reaches at least 85 percent.

Default Configuration

Table 240: Default Configuration for the DiskConsumptionCloseToCapacityThreshold RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error

Value	Default Configuration
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: DiskConsumptionCloseToCapacityThreshold event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DiskConsumptionExceedsCapacityThreshold

This alert is generated when the hard disk usage on the Cisco Unity Connection server meets or exceeds the percentage limit that the **System Settings** > **Advanced** > **Disk Capacity** window in Cisco Unity Connection Administration specifies.

Default Configuration

Table 241: Default Configuration for the DiskConsumptionExceedsCapacityThresholdRTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: DiskConsumptionExceedsCapacityThreshold event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LicenseExpirationWarning

Cisco Unity Connection licenses several features, including users and ports. The system enforces these licenses. If a customer uses a time-limited license to sample a feature, this license includes an expiration date. Before the license expiration date is reached, the system sends a message, and this alert occurs. The log indicates how many days remain until the license expires.

Default Configuration

Table 242: Default Configuration for the LicenseExpirationWarning RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: LicenseExpirationWarning event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LicenseExpired

Cisco Unity Connection licenses several features, including users and ports. The system enforces these licenses. If a customer uses a time-limited license to sample a feature, this license includes an expiration date. When the license expiration date is reached, the license becomes invalid, and this alert occurs.

Default Configuration

Table 243: Default Configuration for the LicenseExpired RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational

Value	Default Configuration
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: LicenseExpired event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

System Error Messages

System Error Messages

For a complete list of system error messages, see the *System Error Messages for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-system-message-guides-list.html.