Cisco Unified Serviceability Alarms and Cisco Log Messages

This chapter describes the Cisco Unified Serviceability alarms and error messages and CiscoLog message format. Network alarms tracked by Cisco Unified Serviceability for Cisco Unified Communications Manager generate the error messages.

Note A History table lists Cisco Unified Serviceability error messages that have been added, changed, or removed beginning in Cisco Unified Communications Manager Release 7.0(1).

Cisco Unified Serviceability Alarms and CiscoLog Messages

Cisco Unified Serviceability alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system. The alarm or error message information includes the application name, machine name, and recommended action and other critical information to help you troubleshoot.

You configure the alarm interface to send alarm information to multiple locations, and each location can have its own alarm event level (from debug to emergency). You can direct alarms to the Syslog Viewer (local syslog), SNMP traps, Syslog file (remote syslog), SDI trace log file, SDL trace log file (for Cisco Unified CM and CTIManager services only), or to all destinations.

You use the Trace and Log Central option in the Cisco Unified Real-Time Monitoring Tool (RTMT) to collect alarms that get sent to an SDI or SDL trace log file. To view the alarm information sent to the local syslog, use the SysLog Viewer in RTMT.

Note All the alarms are logged based on their severity and settings of alarm event level. For information on viewing the alarm configuration settings, refer to the *Cisco Unified Serviceability Administration Guide*.

CiscoLog Format

CiscoLog, a specification for unified logging in Cisco software applications, gets used in the Cisco Unified RTMT. It defines the message format when messages are logged into file or by using the syslog protocol. The output that is provided by Cisco software applications gets used for auditing, fault-management, and troubleshooting of the services that are provided by these applications.

Be aware that CiscoLog message format is compatible with one of the message formats that is produced by Cisco IOS Release 12.3 by using the syslog protocol when Cisco IOS Software is configured with the following commands:

- **service sequence-numbers—**A default sequence number that is produced by Cisco IOS. An additional sequence number can also be enabled with this command. This command forces sequence numbers to be shown in terminal output, but results in two sequence numbers in the syslog output. CiscoLog standardizes on a format with just one sequence number. Thus, the compliant Cisco IOS Software configuration occurs when the second number is disabled by using the no service sequence-numbers command.
- **logging origin-id hostname—**The CiscoLog HOST field remains consistent with that produced by the Cisco IOS Release 12.3 when configured with this command. This command does not get documented in the Cisco IOS Software documentation but is available in Cisco IOS Release 12.3. CiscoLog stays compatible with the results that Cisco IOS Software produces in this field.
- **service timestamps log datetime localtime msec show-timezone year—**The CiscoLog TIMESTAMP field remains consistent with the timestamp format produced by Cisco IOS Release 12.3 when configured with this command.

Note CiscoLog uses the same field delimiters as Cisco IOS Software Release 12.3.

Log File and Syslog Outputs

When CiscoLog messages are written directly into a log file by an application, each message is on a separate line. The line separator should be a standard line separator used on a given platform. On Windows, the line separator must be the sequence of carriage return and line feed characters (ASCII decimal values 13 and 10; often designated as "\r\n" in programming languages). On Solaris and Linux, the line separator is a single line

feed character (ASCII decimal value 10 and in programming languages typically "\n"). Two line separators must never appear one after another, for example, you cannot have "\r\n\r\n" on Windows, but "\r\n" is fine because these two characters are a single line separator.

In practical terms, this means that applications should be careful when appending data to an existing log. In some cases an initial line break is required and in others not. For example, if application crashes when writing CiscoLog message, but before it wrote a line break to file, then when the application starts up, it should print an initial line break before printing the next message. An application can determine if an initial line break is necessary during startup by checking the last character sequence in the log file that will be used for appending.

CiscoLog message format is identical for messages written directly to a log file or those generated by using the syslog protocol with two minor exceptions. When CiscoLog messages are written directly into to a file they must be appended with line separators. When CiscoLog messages are sent by using the syslog protocol then the syslog RFC 3164 protocol PRI header must be prepended to each CiscoLog message.

The syslog PRI field encodes syslog message severity and syslog facility. The severity encoded in the PRI field must match the value of the CiscoLog SEVERITY field. Any syslog facility can be used regardless of the content of the message. Typically, a given application is configured to send all its messages to a single syslog facility (usually RFC 3164 facilities local 0 through local 7). Refer to RFC 3164 for details about how to encode the PRI field. Below is an example of a CiscoLog message with the syslog protocol PRI field <165> which encodes the severity level of notice (5) and facility value local4.

```
<165>11: host.cisco.com: Jun 13 2003 12:11:52.454 UTC: %BACC-5-CONFIG: Configured from
console by vty0 [10.0.0.0]
```

Messages as shown in the example above can be sent to UDP port 514 if using RFC 3164 logging mechanism.

Syslog RFC 3164 provides additional guidelines for message content formatting beyond the PRI field. However, RFC 3164 is purely information (not on IETF standards track) and actually allows messages in any format to be generated to the syslog UDP port 514 (see section 4.2 of RFC 3164). The RFC provides observation about content structure often encountered in implementations, but does not dictate or recommend its use. CiscoLog format does not follow these observations due to practical limitations of the format defined in the RFC. For example, the time stamp is specified without a year, time zone or milliseconds while the hostname can only be provided without the domain name.

CiscoLog messages must remain unaltered when relayed. The PRI field is not part of a CiscoLog message, but rather a protocol header. It can be stripped or replaced if necessary. Additional headers or footers can be added to and stripped from the CiscoLog message for transport purposes.

Standard Syslog Server Implementations

Standard syslog server implementations can be configured to forward received log messages or to store the messages locally. Most syslog server implementations strip the PRI field from the received messages and prefix additional information to the message before storage. This additional information typically includes two extra fields: the local time stamp and the host identifier (IP or DNS name) of the server, which generated or relayed the message.

The following example of a CiscoLog message shown the output after being logged by the Solaris 8 syslog server:

```
Jun 13 12:12:09 host.cisco.com 11: host.cisco.com: Jun 13 2003 12:11:52.454 UTC:
%BACC-5-CONFIG: Configured from console by vty0 [10.0.0.0]
```

There is no standard that defines how syslog servers must store messages. Implementations vary greatly. CiscoLog only addresses the format in which messages are sent to the syslog server, not how they are stored by the server that receives them. Specifically, the format and presence of any additional header fields in syslog log files is outside of the scope of this specification.

Note The CiscoLog specification recommends that the syslog server implementation store CiscoLog messages in exactly the same format as it receives them only stripping the PRI field and without any extra headers. This would provide an identical storage format for CiscoLog messages written directly to the log file by an application or logged through syslog protocol.

Clock Synchronization

It is important that the clocks of all hosts of a distributed application be synchronized with one authoritative clock. This can be accomplished by using protocols such as NTP. Clock synchronization is recommended because the time stamps in log messages are required in order to be able to reconstruct the correct sequence of events based on messages originating from multiple processes or multiple hosts. Clock drifts can still occur, but ongoing synchronization should reduce this issue to a minimum.

Multipart Messages

ASCII control characters are not permitted in any of the fields of CiscoLog message format. Control characters include characters such as line feed, form feed and carriage returns. This means that multi-line messages are not allowed unless to allow:

- Better presentation (for example, a stack trace)
- Fragmenting messages which exceed 800 octet limit

Multi-part CiscoLog message consists of a set of multiple valid CiscoLog messages. Messages are grouped together using a special tag key “part”, which identifies the part number and the sequence number of the original message.

All messages which are part of a multi-part message must have a “part” tag as well as identical values for the HOST, TIMESTAMP, APPNAME, SEVERITY fields and other TAG values. However, the sequence number of each message has to be incremented as usual.

Example of a multi-part message:

```
16: host.cisco.com: Jun 13 2003 23:11:52.468 UTC:
%BACC-3-UNEXPECTED_EXCEPTION: %[pname.orig=rdu][part=16.1/3]: Null pointer
 exception
17: host.cisco.com: Jun 13 2003 23:11:52.468 UTC:
%BACC-3-UNEXPECTED_EXCEPTION: %[pname.orig=rdu][part=16.2/3]:
com.cisco.Source:123
18: host.cisco.com: Jun 13 2003 23:11:52.468 UTC:
%BACC-3-UNEXPECTED_EXCEPTION: %[pname.orig=rdu][part=16.3/3]:
com.cisco.Main:1112
```

In this example, the first message has part number 1 and its sequence number, 16, embedded in the part tag. Subsequent messages embed the sequence number of the first message part and provide their own part number. The trailing “/3” in each part tag value means that the message consists of three parts.

CiscoLog Message Format

The CiscoLog message format follows:

<SEQNUM>: <HOST>: <TIMESTAMP>: %<HEADER>: [TAGS:]<MESSAGE>

All fields gets separated by a single colon character (ASCII decimal value 58) and a single space character (ASCII decimal value 32). The HEADER field is also preceded by a percent character (ASCII decimal value 37).

The TIMESTAMP, HEADER and TAGS fields have internal formatting. Below is a complete format with details for TIMESTAMP and HEADER fields:

<SEQNUM>: <HOST>: [ACCURACY]<MONTH> <DAY> <YEAR>
<HOUR>:<MINUTES>:<SECONDS>.<MILLISECONDS> <TIMEZONE>:
%<APPNAME>-<SEVERITY>-<MSGNAME>: [TAGS:]<MESSAGE>

All fields except for ACCURACY and TAGS are required.

The following example shows a CiscoLog message:

```
11: host.cisco.com: Jun 13 2003 23:11:52.454 UTC: %BACC-5-CONFIG: Configured from
console by vty0 [10.10.10.0]
```

The following example shows the optional TAGS and ACCURACY fields in a CiscoLog message:

```
12: host.cisco.com: *Jun 13 2003 23:11:52.454 UTC: %BACC-4-BAD_REQUEST:
%[pname.orig=rdu][comp=parser][mac=1,6,aa:bb:cc:11:22:33][txn=mytxn123]: Bad request
received from device [1,6,aa:bb:cc:11:22:33]. Header missing.
```

The values of the specific fields in the above example are as follows:

- SEQNUM – “12”
- HOST – “host.cisco.com”
- ACCURACY – “*”
- MONTH - “Jun”
- DAY – “13”
- YEAR – “2003”
- HOUR – “23”
- MINUTES – “11”
- SECONDS – “52”
- MILLISECONDS – “454”
- TIMEZONE – “UTC”
- APPNAME – “BACC”
- SEVERITY – “4”
- MSGNAME – “BAD_REQUEST”
- TAGS – “%[pname.orig=rdu][comp=parser][mac=1,6,aa:bb:cc:11:22:33][txn=mytxn123]”
- MESSAGE – “Bad request received from device [1,6,aa:bb:cc:11:22:33]. Header missing.”

Message Length Limit

The maximum length of a complete CiscoLog message must not exceed 800 octets.The term octet is used for 8-bit data type instead of byte because byte is not 8 bits on some platforms. The words “character” and “octet” are not synonyms in parts of this specification because in places were internationalization is supported a single character may need to be represented with multiple octets. This limit is dictated by RFC 3164. The limit of

1024 octets reserves some extra space for syslog forwarding headers and/or fields that may be formalized in later specifications.

When CiscoLog message includes the syslog PRI field, then the combined CiscoLog messages and PRI field length must not exceed 805 octets.

SEQNUM Field

The SEQNUM field contains a sequence number, which can be used to order messages in the time sequence order when multiple messages are produced with the same time stamp by the same process. The sequence number begins at 0 for the first message fired by a process since the last startup and is incremented by 1 for every subsequent logging message originated by the same process. Every time the application process is restarted, its sequence number is reset back to 0. The sequence number of each message must be in the exact order in which messages are fired/logged by the application.

This may mean that in a multi-threaded application there must be some kind of synchronization to ensure this and another consideration may have to be made for Java applications that have some native (C) code in JNI. If log messages originate in both native and Java parts of the same process, the implementation needs to be synchronized to use the same sequence number counter across the two process parts and to fire messages in the order of sequence numbers.

The maximum numeric value of the SEQNUM field is 4,294,967,295 at which point the counter must be reset back to 0. The maximum positive value of a 32-bit unsigned integer as used in Cisco IOS. Cisco IOS uses ulong for the sequence number counter and ulong is a 32-bit unsigned integer on all current Cisco IOS platforms including mips, ppc, and 68k.

Sequence numbers are process specific. If application architecture has multiple application processes on a single host, which share a single logging daemon, the sequence number still has to be process-specific. Thus, each process has it is own sequence number which it increments.

Sequence numbers also help detect lost messages. Therefore, sequence numbers cannot be skipped. In other words, a message must be produced for every number in the sequence order.

HOST Field

The HOST field identifies the system originating the message with a Fully Qualified DNS Name (FQDN), hostname or an IPv4/IPv6 address. If the FQDN or hostname is known, one of the two has to appear in the HOST field. It is expected that in most deployments the hostname is sufficient. However, if a deployment spans multiple domains, then using FQDNs is recommend. If an application is expected to be deployed in both scenarios, then it is recommended that the application default to the FQDNs, but make it a configurable option.

If neither FQDN nor hostname can be identified, then the IP address of the host must be used. If the IP address cannot be identified, then a constant “0.0.0.0” (without quotes) must appear in place of the HOST field.

Note With regards to the compliance with Cisco IOS format. Cisco IOS Release 12.3 supports producing hostname, IP address, or any user-defined string in the HOST field. If it is configured to provide a hostname and it is not set on the device, it will use a string such as “Router.”

The length of the HOST field must not exceed 255 octets.

FQDN and Hostname

If multiple FQDNs or hostnames are known for a given system, applications must use the primary FQDN/hostname or an arbitrary one if no primary is designated. However, applications must use the same HOST field value until some relevant configuration change takes place. In other words, the FQDN/hostname value should not arbitrarily change from message to message if system is configured with multiple FQDNs/hostnames.

Only printable US ASCII characters (those with decimal values 32-126) and foreign language characters are allowed in the HOST field when encoding an FQDN or hostname. The appropriate character set and encoding for HOST should be compliant with RFC 1123 / STD-3.

The acceptable character set per these standards includes US ASCII letters, numbers, dash and dot separator characters (although not starting or ending with a dash). The reason that these are only recommendations of adhering to these standards is that, in practice, many hosts do not follow the convention and use characters such as underscore in the hostname. However, the HOST field cannot contain a character sequence of ": " (colon and space) as this sequence is used as a field delimiter in the CiscoLog format.

Foreign language characters outside of the printable US ASCII characters have to be encoded according to internationalization rules.

Use of non-printable (control) ASCII characters is not allowed in the HOST field. Control characters include characters with ASCII decimal values 0-31 and 127. If an application provides a CiscoLog-compliant library with a host string, which includes one or more control characters, the logging library must do the following. If the horizontal tab character (ASCII decimal value 9) is encountered, it must be replaced with one or more space characters (ASCII decimal value 32). Eight spaces per tab are recommended because this is a convention on most Unix and Windows platforms. Other control characters must each be replaced with a question mark character (ASCII decimal value 63).

While DNS is letter-case agnostic, CiscoLog places an additional recommendation of using only lower-case characters in the HOST field for ease of readability. The use of the trailing dot at the end of the FQDN is optional. The following examples are valid HOST fields:

- host123
- host-123
- host123.cisco.com
- host123.cisco.com.

IP Addresses

The IP address value used in the HOST field can be either an IPv4 or IPv6 address. If a device has multiple IP addresses, the primary IP address of the device must be used regardless of the interface through which the CiscoLog message is sent to syslog server. If no primary IP address is designated, a fixed/static IP address is preferred to a dynamically assigned one. If multiple static IP addresses exist, any one can be used, but it must be used consistently in all messages until a relevant configuration event occurs on the system.

- IPv4 Address—IPv4 address should be represented in dot notation "x.x.x.x", where x is a decimal value from 0 to 255 encoded as ASCII text. If an IP address is unknown, "0.0.0.0" (without quotes) must be used as a place holder. Examples of valid IPv4 addresses are 0.0.0.0 and 212.1.122.11.

  Below is an example of a message with an IPv4 address in the HOST field:

```
11: 212.1.122.11: Jun 13 2003 23:11:52.454 UTC:
%BACC-3-BAD_REQUEST: Bad request received from device [1.2.3.4]. Missing header.
```

Below is an example of a CiscoLog message when FQDN, hostname or IP are all unknown:

```
11: 0.0.0.0: Jun 13 2003 23:11:52.454 UTC:
%BACC-3-BAD_REQUEST: Bad request received from device [1.2.3.4]. Missing header.
```

- IPv6 Address—IPv6 address representation must follow conventions outlined in RFC 3513, sections 2.2.1, 2.2.2 and 2.2.3. Specifically, all three conventions are supported. Both lower-case and upper-case letters can be used in the IPv6 address, but the lower-case letters are recommended. If an IP address is unknown, “0.0.0.0” (without quotes) should be used as the IP address. Examples of valid IPv6 addresses:
  - 1080:0:0:800:ba98:3210:11aa:12dd (full notation)
  - 1080::800:ba98:3210:11aa:12dd (use of “::” convention)
  - 0:0:0:0:0:0:13.1.68.3 (last 4 octets expanded as in IPv4)
  - 0.0.0.0 (unknown FQDN, hostname and IP address)

Below is an example of a message with an IPv6 address in the HOST field:

```
11: 1080:0:0:800:ba98:3210:11aa:12dd: Jun 13 2003 23:11:52.454 UTC:
%BACC-3-BAD_REQUEST:  Bad request received from device [1.2.3.4]. Missing header.
```

TIMESTAMP Field

The TIMESTAMP field provides date with year, time with milliseconds and a time zone identifier in the following format:

[ACCURACY]<MONTH> <DAY> <YEAR> <HOUR>:<MINUTES>:<SECONDS>.<MILLISECONDS> <TIMEZONE>

Below are several examples of valid time stamps:

```
Jun 13 2003 23:11:52.454 UTCJun  3 2003 23:11:52.454 UTC
Jun 22 2003 05:11:52.525 -0300
*Feb 14 2003 01:02:03.005 EST
```

In some cases, it is possible that a device may not have the knowledge of the date and/or time due to hardware or software limitations. In such circumstances, the following string must be produced TIMESTAMP field: "--- 00 0000 00:00:00.000 ---". Below is an example of a CiscoLog message from a device which has no knowledge of date and/or time:

```
11: host.domain.com: --- 00 0000 00:00:00.000 ---: %BACC-3-BAD_REQUEST: Bad request received
 from device [1.2.3.4]. Missing header.
```

Devices which are not aware of their clock, may choose to provide an uptime as a relative measure of time. If device is capable of providing uptime, it is recommended that does so as a substitute for unavailable time stamp. If uptime is provided it must be provided with a standard uptime tag as outlined in the CiscoLog Standard Tags specification.

The following table details each field specification.

Table 1: TIMESTAMP Field Specifications

Field	Specification
ACCURACY	This is an optional field. If present, it must be either a single asterisk character (ASCII decimal value 42), or a single dot character (ASCII decimal value 46). No separator character is used after this field. This field indicates the status of clock synchronization. Cisco IOS uses a special convention for time prefixes to indicate the accuracy of the time stamp. If dot character appears before the date, it means that the local time was synchronized at some point via NTP, but currently no NTP servers are available. The asterisk character in front of the date means that the local time is not authoritative, i.e. NTP servers are not setup.
	CiscoLog supports the use of this convention, but does not require it. If an application is integrated with NTP client software, and knows that its time is out of sync, then it can optionally prefix the message with asterisk character. However, because applications may choose not to use this scheme, the lack of "." or "*" in CiscoLog messages should not be interpreted to mean that the local time is synchronized.
MONTH	Must be one of the following three-character month designations followed by a single space (ASCII decimal value 32) as a delimiter character: Jan, Feb, Mar, Apr, May, Jun, Jul, Sep, Oct, Nov or Dec.
DAY	Must consist of two characters. If day is a single digit, it must be prefixed with a single space character. The acceptable range of values is from 1 to 31. The day value must be followed by a single space as a delimiter character.
YEAR	Must consist of exactly 4 digit characters followed by a space as a delimiter character.
HOUR	Must consist of exactly two number characters. The hour value is based on a 24-hour clock. Values range from 00 to 23. If hour value is a single digit, it must be prefixed with a single zero character. The hour value must be followed by a single colon as a delimiter character.
MINUTES	Must consist of exactly two number characters. Values range from 00 to 59. If minute value is a single digit, it must be prefixed with a single zero character. The minutes value must be followed by a single colon as a delimiter character
SECONDS	Must consist of exactly two number characters. Values range from 00 to 59. If seconds value is a single digit, it must be prefixed with a single zero character. The seconds value must be followed by a period as a delimiter character.
MILLISECONDS	Must consist of exactly 3 digit characters. Values range from 000 to 999. If milliseconds value is less then 3 digits in length it must be prefixed with extra zeros to make it a 3-character field. The milliseconds value is followed by a space as a delimiter character.

Field	Specification
TIMEZONE	Must consist of at least one, but no more than 7 characters in the following ASCII decimal value range: 32-126. The value must not include a combination of colon-space-percent of characters – ": %" (ASCII decimal values 58, 32, 37) – as this character combination is reserved as a field delimiter that follows the time stamp. There is no standard set of acronyms for time zones[1]. A list of common time zone acronyms and corresponding time offsets from UTC is provided in the UTC specification. Uppercase letters are recommended for time zone acronym values. CiscoLog recommends the use of time offset instead of time zone identifier in this field. The offset, if provided, must follow the following format "-hhmm" or "+hhmm" to indicate hour and minute offset from UTC. In this format time zone field must always contain 5 characters, with the last 4 characters being constrained to numbers only. Unlike a textual time zone identifier, this format provides a specific time offset from universal standard time. Cisco IOS Release 12.3 supports any 7-character string as a time zone identifier, so it can be configured in a way which is compatible with this recommendation. Multiple messages may and sometimes must be produced with exactly the same time stamp. This can happen naturally on a non-preemptive operating system or may need to be deliberately induced as in the case of multi-part messages. Sequence numbers then become helpful for establishing message order. Time stamp should always be accurate to the millisecond unless it can significantly hinder performance of the application. In either case, applications must always provide the administrator with an option to output messages with exact time stamp in milliseconds. If an application uses time stamp with accuracy to the second (instead of a millisecond), it must put the last known milliseconds value or 000 in place of the milliseconds. Whatever convention is chosen by the application, it should be followed consistently.

1

[2]

HEADER Field

The HEADER field has the following format:

<APPNAME>-<SEVERITY>-<MSGNAME>

A single dash character (ASCII decimal value 45) serves a separator for the three fields.

2 Neither Cisco IOS nor CiscoLog define a standard set of time zone acronyms because there is no single established standard.

APPNAME Field

The APPNAME field in the HEADER defines the name of the application producing the message. Cisco IOS uses FACILITY in place of APPNAME that names the logical component producing the message. Cisco IOS 12.3 defines approximately 287 facilities for 3950 messages. Example of some easily recognizable facilities: AAAA, SYS, ATM, BGP, CRYPTO, ETHERNET, FTPSERVER, CONFIG_I, IP, ISDN, RADIUS, SNMP, SYS, TCP, UBR7200, X25. A complete list of defined facilities is available in Cisco IOS documentation at http://.

Outside of the Cisco IOS, there can be multiple applications on the same host originating log messages. Therefore, it is necessary that APPNAME field identify the specific application. Additional source identifiers are available in the HOST field as well as various standard TAGS field values (pname, pid, comp, etc).

The APPNAME field must consist of at least two uppercase letters or digits and may include underscore characters. More precisely, the acceptable character set is limited to characters with the following ASCII decimal values: 48-57 (numbers), 65-90 (upper-case letters) and 95 (underscore).

The length of the APPNAME field must not exceed 24 characters.

Application names cannot conflict with other Cisco software applications and with Cisco IOS facilities.

On the Solaris platform, it is recommended (not required) that the application name values used in the APPNAME field be consistent with those used for the application installation package name, only in upper case and without the CSCO prefix. For example, an application registering as “CSCObacc” on Solaris should use “BACC” as the value of the APPNAME field.

Some applications may choose to specify a version as part of the APPNAME field. This is acceptable and may be useful in cases where the meaning of certain messages is redefined from one release to another. For example, an APPNAME value could be “BACC_2_5” for BACC version 2.5. The use the version within an application name is optional and may be introduced by applications in any release.

SEVERITY Field

The SEVERITY field is a numeric value from 0 to 7, providing eight different severities. The severities defined below match Cisco IOS severity levels. They are also standard syslog severities.

It is important that messages use the correct severity. An error in a certain component may be severe as far as the component is concerned, but if the overall application handles it gracefully, then the severity may be lower for the application as a whole. The following table lists guidelines that should be followed in determining the severity of a message.

Table 2: Name and Severity Level and Descriptions in Error Messages

Name/Severity Level	Description
Emergency (0)	System or service is unusable. Examples: • Service repeatedly fails to startup • System ran out of disk space while disk space is essential for this system to operate • Application requires root privileges to run but does not have them

Name/Severity Level	Description
Alert (1)	Action must be taken immediately. Examples: • Application is about to run out of licenses • Application is about to run out of disk space • Too many unauthorized access attempts detected • Denial of service attack is detected
Critical (2)	Critical condition. Similar to alert, but not necessarily requiring an immediate action. Examples: • Received an invalid authentication request • Service crashed due to an error that could not be handled, like an out of memory condition, (provided it has a watchdog process to restart it, it does not necessarily require immediate action) • Unexpected code error that could not be handled
Error (3)	An error condition, which does not necessarily impact the ability of the service to continue to function. Examples: • Problem parsing/processing a particular request which does not prevent the application from handling other requests • Unexpected, but handled code exception
Warning (4)	A warning about some bad condition, which is not necessarily an error. Examples: • Lost network connection to some resource • Timed out waiting for a response
Notice (5)	Notifications about system-level conditions, which are not error conditions. Examples: • Configuration was updated (not audit level information) • Process has started • Process is shutting down gracefully on request

Name/Severity Level	Description
Informational (6)	Informational messages are distinguished from notification in that they provide information for internal flows of the application or per-request information instead of system-wide notifications. Informational messages are used for troubleshooting by users who are familiar with the basic flows of the application. Examples: • Request received • Request was parsed successfully • Request being processed • Response sent back • Acknowledgement received • Detailed audit information
Debug (7)	Debugging messages are similar to informational messages, but provide more detail and require the user to have better knowledge of system internal processing. These messages are typically reserved for very advanced users or Cisco technical support. Examples: • Complete details for a request packet • Internal state machine state changes • Internal profiling statistics • Internal events

If an application uses a default severity level to determine which messages should be logged, then it is recommended that this level be set at 5 (notice). This ensures that all messages of severity 5 or higher are logged by default.

MSGNAME Field

The MSGNAME field of the HEADER uniquely identifies the message within the context of a given APPNAME. A fixed severity and logical meaning is associated with a specific MSGNAME within a specific APPNAME. In other words, the same message name cannot appear with different severity or a completely different logical meaning for the same APPNAME value even if the message is originated by a different process.

Message names are only unique within a given application (a given APPNAME value) unless the message is one of the standard messages. Thus, applications interpreting CiscoLog messages should be careful not to assume that a message with a given name has the same meaning for all applications that may use this message name. Indeed, if the message is not one of the standard messages, it may have a different severity and meaning in a different application.

The MSGNAME field must consist of at least two characters. Acceptable characters are limited to the following ASCII decimal values: 48-57 (numbers), 65-90 (upper-case letters) and 95 (underscore). While IOS allows lower-case letters as well, the vast majority of IOS messages use only the upper-case letters. In order to be

consistent with established conventions we opted to restrict the character set to upper-case letters, numbers and underscore characters.

Both numeric-only or alphanumeric message names are acceptable. However, per IOS convention, it is recommended that a user-friendly alphanumeric label be preferred to a numeric-only label. For example, “NO_MEMORY” message name is preferred to a “341234” identifier.

A special tag *mid* is defined in the CiscoLog Standard Tags specification for identifying a numeric id corresponding to a message name. This tag can be used to provide a numeric message is in addition to the MSGNAME. When this tag is used, a given MSGNAME must always correspond to a single message id value. CiscoLog defines *mid* tag values for each standard message.

The length of the MSGNAME field must not exceed 30 characters, but most message names should be more concise. MSGNAME value may not conflict with the names defined in this standard.

A separate message name must be defined for each logically different message. In other words, while the message text for a given message name can vary by virtue of some substitutable parameters, logically different messages must have different message names.

The following is an example of correct use of message name:

```
11: host.cisco.com: Jun 13 2003 23:11:52.454 UTC: %BACC-4-CONNECTION_LOST: %[pname.orig=rdu]:
 Server lost connection to host [1.1.1.1]12: host.cisco.com: Jun 13 2003 23:11:52.458 UTC:
 %BACC-4-CONNECTION_LOST: %[pname.orig=rdu]: Server lost connection to host [2.2.2.2
```

Notice that while the IP address of the host changes, it is still logically the same type of message. The following is an example of an **INCORRECT** use of the message name:

```
15: host.cisco.com: Jun 13 2003 23:11:52.458 UTC: %BACC-4-CONNECTION: %[pname.orig=rdu]:
Server lost connection to host [2.2.2.2]16: host.cisco.com: Jun 13 2003 23:11:52.468 UTC:
%BACC-4-CONNECTION: %[pname.orig=rdu]: Server re-established connection to host [2.2.2.2]
```

The use of a single message name for two different events in the above example is wrong and unacceptable. This is referred to as a “catch-all” message name and they must be avoided. Another extreme example is defining a message named “ERROR” and providing all error log messages under the same message name. This defeats the purpose of having the message name field, which is to enable external filtering of messages or easily trigger actions.

The only exception to the “no-catch-all” rule is when message cannot be identified ahead of time with anything better than a generic description or the users will not benefit from distinguishing the various subtypes of the message.

Although some applications may choose to do so, there is generally no need to define a separate message name for all debugging messages because debugging messages are not intended for automated filtering and action triggering based on message name. The sheer number of debugging messages and the highly dynamic nature of what is produced in them makes it very hard to define separate messages.

This specification proposes establishing a mailing list that could be used by groups for consulting purposes when in doubt about how to define certain messages. Currently, the mailing list alias used for this purpose is “cmn-logging”.

TAGS Field

The TAGS field is optional in the message format. It provides a standard mechanism for applications to provide structured content in the form of key-value pairs which can be used to categorize or filter a set of messages externally.

Tags can be used to identify virtual logging channels. A set of messages flagged with the same tag can later be grouped together. For example, an application may flag messages belonging to a particular thread by supplying the corresponding tag. This would then allow filtering and viewing messages based on threads.

Virtual logging channels can also be established across multiple applications. For example, if all applications could tag requests from a device with device id (mac, ip, etc), then it would be easy to filter all messages related to that device even thought it communicates with multiple components.

Each application may define its own set of supported tags. A single tag consists of key and value pair separated by the equals sign and surrounded by square bracket characters as in the following format: [KEY=VALUE]. This is an example of a valid tag key-value pair [ip=123.23.22.22].

The TAGS field is prefixed with a percent character (ASCII decimal value 37) and ends with a sequence of colon and space characters (ASCII decimal values 58 and 32). When multiple tags are assembled together, no characters should appear between the tags as separators. The following example has a complete CiscoLog message with four tags:

```
12: host.cisco.com: Jun 13 2003 23:11:52.454 UTC: %BACC-4-BAD_REQUEST:
%[pname.orig=rdu][comp=parser][mac=1,6,aa:bb:cc:11:22:33][txn=mytxn123]: Bad request received
 from device [1,6,aa:bb:cc:11:22:33]. Missing header.
```

If TAGS field is missing, the percent character prefix and the trailing colon and space must be omitted. Thus, when the TAGS field is missing, the HEADER and MESSAGE fields must be separated by just a single colon and a space which follows the HEADER field. For example:

```
12: host.cisco.com: Jun 13 2003 23:11:52.454 UTC: %BACC-4-BAD_REQUEST: Bad request received
 from device [1,6,aa:bb:cc:11:22:33]. Missing header.
```

Multiple tags with the same tag key can be provided in the same message. This essentially provides the capability for handling multi-valued keys. Below is an example of a message produced from a device which has two IP addresses where the application chose to provide both IP addresses in the TAGS field as well as the process name:

```
12: host.cisco.com: Jun 13 2003 23:11:52.454 UTC: %BACC-4-BAD_REQUEST:
%[pname.orig=rdu][ip.orig=1.1.1.1][ip.orig=1.1.1.2]: Bad request received from device
[1,6,aa:bb:cc:11:22:33]. Missing header.
```

Any number of tags can be provided in a given message. The only limit is the overall length limit of the CiscoLog message of 800 octets.

If multiple tags are present, it is recommended that they appear in the alphanumeric order of the keys. This insures that tags are always produced in the same order. However, a different order may be chosen by an application if the order of tags is used to communicate some semantic value.

Tag Keys

Tag key must contain at least one character. The characters are limited to ASCII characters with decimal values 48-57 (numbers), 65-90 (upper-case letters), 95 (underscore), 97-122 (lower case letters). Use of lower-case letters is recommended. There is no strict limit on tag key length, although a general message limit of 800 octets applies and dictates that one should attempt to define short tag key names.

Tag Semantic Extensions

In some cases, a tag can have a standard value syntax, but different meaning depending on the content in which it is used. Tag semantic extensions are used to differentiate the contextual meaning of tags.

The semantic extension tags are created by appending the tag key with a single dot character (ASCII decimal value 46) and a text string consisting of characters from a proper character set.

For example, an “ip” tag defines syntax for an IP address representation, but no semantic value. An “ip” tag found in a CiscoLog message generally means only that this IP address is somehow related to the message. In some cases, such vague association is sufficient. However, sometimes, communicating semantic value could be useful.

A message may have two IP address tags associated with it, for example, from and to IP addresses. In this case, using tags “ip.from” and “ip.to” would communicate both the syntax of the tags and some semantic value. Another example, is a standard tag “ip.orig”, which specifies the IP address of the host which originated the message. The following is an example of all three tags appearing together:

```
[ip.from=1.1.1.1][ip.to=2.2.2.2][ip.orig=123.12.111.1]
```

Multiple levels of semantic extension tags are allowed with each extension providing meaning that is more specific. For example, tag key “ip.to.primary” is valid and could mean the primary IP address of the destination host.

The semantic value is much harder to standardize than the syntax because there can an infinite number of meanings for a given value depending on the context. Thus, it is anticipated that defining tag semantics extensions will be largely application specific.

Tag Values

Tag values may contain zero or more characters. The empty (zero characters) value is interpreted as unknown or undetermined value. The value must only include printable US ASCII characters (those in the ASCII decimal value range 32-126) and foreign language characters

There is a restriction on the use of three characters: “[“,”]” and “\”. The bracket characters (ASCII decimal values 91 & 93) must be escaped with a back slash character (ASCII decimal value 92) . This helps to avoid confusion with the brackets that signify the start/end of the tag. Thus, when the tag value needs to represent characters “[“ or ”]”, a sequence of “\[“ or ”\]” is used instead respectively. When the escape character itself needs to be represented in the tag value, then instead of the “\” character a sequence of “\\” is used.

Use of non-printable (control) ASCII characters is not allowed in the TAG value field. Control characters include characters with ASCII decimal values 0-31 and 127. If application provides to a CiscoLog-compliant library a tag value string, which includes one or more control characters, the logging library must do the following. If the horizontal tab character (ASCII decimal value 9) is encountered, it must be replaced with one or more space characters (ASCII decimal value 32). Eight spaces per tab are recommended because this is a convention on most Unix and Windows platforms. Other control characters must each be replaced with a question mark character (ASCII decimal value 63). Technically, we only need to require escaping a closing bracket. However, requiring escaping both open and closing brackets simplifies parser code and provides for a more consistent display in raw form.

There is no strict limit on tag value length; although a general message length limit of 800 octets applies and dictates that one must be conservative.

Tag Guidelines

The TAGS field is optional in the CiscoLog message format. Tags do not replace substitutable parameters in the message body. Tags merely provide an additional way to identify and categorize messages.

Since tags are optional, they can be enabled or disabled by the application/user as required. There is no requirement for the same message to always be produced with the same set of tags. If the application supports a given tag, it does not necessarily mean that it must always produce it. This can be configurable. Indeed, it is recommended that applications provide the administrator with at least limited control over which tags get produces.

Application developers have a choice as to what information to make available in the tags and what in the message body. In some cases, the information may be duplicated between the two. This is acceptable.

The general guideline is to put all required information in the message body and make appropriate information available via tags. In other words, the message should provide sufficient meaning even when all tags are

disabled. Tags merely provide additional useful information and a way to present it in a standard, easily filtered, form.

The following are two valid examples of a message where both the message and the message tags contain a MAC address. Example with tags disabled:

```
11: host.cisco.com: Jun 13 2003 23:11:52.454 UTC: %BACC-3-BAD_REQUEST: Bad request received
 from device [1,6,aa:bb:11:22:33:aa]. Missing header.
```

In the above example, the MAC address appears as part of the message field – it is not a tag. In the following example, the tags are enabled. Even though MAC address is duplicated between the tag and the message, it is acceptable.

```
11: host.cisco.com: Jun 13 2003 23:11:52.454 UTC: %BACC-3-BAD_REQUEST:
%[mac=1,6,aa:bb:11:22:33:aa][tid=thread1][txn=mytxn123]: Bad request received from device
[1,6,aa:bb:11:22:33:aa]. Missing header.
```

Process Identification Tag

One of the standard tags, pname.orig, is used to identify the logical process name which originates the message. Any application that seeks to provide originating process information must do so using the “pname.orig” tag.

This tag is extremely valuable in addition to information in the APPNAME field because some applications consist of multiple processes, each of which may originate logging messages. It is recommended that any application which consists of multiple processes always provide the “pname.orig” tag.

MESSAGE Field

The MESSAGE field provides a descriptive message about the logging event. This field may consist of one or more characters. The character set is limited to printable US ASCII characters (ASCII decimal values 32-126) and foreign language characters.

Use of non-printable (control) ASCII characters is not permitted in the MESSAGE field. Control characters include characters with ASCII decimal values 0-31 and 127. If application provides a CiscoLog-compliant library with message string, which includes one or more control characters, the logging library must do the following. If the horizontal tab character (ASCII decimal value 9) is encountered, it must be replaced with one or more space characters (ASCII decimal value 32). Eight spaces per tab are recommended because this is a convention on most Unix and Windows platforms. Other control characters must each be replaced with a question mark character (ASCII decimal value 63).

The maximum length of the MESSAGE field is constrained only by the maximum length of the entire message. The maximum length of the CiscoLog message must not exceed 800 octets. Another practical limitation is a potentially highly variable length of the TAGS field.

Message text may contain substitutable parameters, which provide necessary details about the message. For example, the IP address in the following example is a substitutable parameter.

```
11: host.cisco.com: Jun 13 2003 23:11:52.454 UTC: %BACC-3-INVALID_REQUEST: Invalid request
 received from device [1.22.111.222]. Missing header.
```

It is recommended (but not required) that substitutable parameters be surrounded by bracket characters “[“ and ”]” as in the above example. It is further recommended that the message text and values of substitutable parameters do not include bracket characters. When it is not possible to avoid brackets characters in the values of substitutable parameters, it is recommended that the value at least does not include unbalances brackets (like an opening bracket without a closing one). When these recommendations are followed, it would be possible to programmatically extract substitutable parameter values out of a CiscoLog message. However, this recommendation is not a strict requirement.

Message text should be spell-checked. Editorial review is recommended. This includes all messages that can be seen by the customers, even debugging messages.

If the first word of the message is an English word, the first letter should be capitalized. Single sentence messages do not require a period at the end.

Internationalization

Foreign language characters are defined as characters with ASCII decimal values 0-126. Foreign language characters are supported in the HOST field, the value part of the TAGS field and the MESSAGE field.

Foreign language characters must be encoded using the Unicode standard UTF-8. UTF-8 provides encoding for any language without requiring the application to know local encoding/decoding rules for a particular language. In fact, the application encoding the message does not even need to know the language of the message. UTF-8 can encode any Unicode character.

UTF-8 encodes US ASCII characters exactly as they would normally be encoded in a 7-bit ASCII convention. This means that applications interpreting CiscoLog messages can assume that entire messages are encoded in UTF-8. On the other hand, applications producing CiscoLog messages can encode the entire message using US-ASCII 7-bit convention if they are known not to support foreign languages in their products.

Since UTF-8 can encode characters in any language, it is possible to mix and match languages. For example, it is anticipated that a one use-case would be the inclusion of just some parameters in foreign language in an otherwise English message. For example, an English message about user authentication could have a username in Japanese. Similarly, any number of languages can be combined in a CiscoLog message.

In order to take advantage of messages, which include a foreign language, a log viewer capable of interpreting UTF-8 would be necessary. Most likely, the log viewer would also require that the appropriate language fonts be installed on a given system. In a US-ASCII only editor, the user will see garbage for non-US-ASCII characters encoded in UTF-8, but should be able to see all US-ASCII text.

Internationalization support can be readily used with CiscoLog messages written to a local file. Syslog RFC 3164, however, does not currently define foreign language support. Thus, in order to take advantage of internationalization with a syslog server, one would need to use a server implementation, which was tested to correctly relay or store all 8-bits of each octet unchanged. This would ensure that UTF-8 encoded parts of the message retain all their information when foreign languages are used.

In UTF-8, a single character is encoded with one or more octets. The CiscoLog message length limit is specified as 800 octets. Developers must be aware that with foreign languages, the 800-octet length limit may mean fewer than 800 characters. When a message is split into a multi-part message, octets belonging to a single character must never be split into separate lines.

Related Topics

Multipart Messages, on page 4

Versioning

CiscoLog does not provide any versioning information in the message format. Extensions to the format must be made within the restrictions of the format. CiscoLog message formats provides for extensions by way of defining additional tags.

If applications require changes to existing messages, the value of APPNAME can redefine message within the new space. For example, the application version can be appended to the application name as BACC_2_5 for BACC 2.5.

Preconfigured System Alarm Notifications

Preconfigured system alerts appear in the RTMT. See the *Real-Time Monitoring Tool Administration Guide* for information about configuration.

For a complete list of system error messages, see the *System Error Messages* document for your release at the following URL:

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-system-message-guides-list.html

Preconfigured CallManager Alarm Notifications

The following list comprises the preconfigured CallManager alerts in RTMT. Refer to the Real-Time Monitoring Tool Administration Guide for information on configuration.

Related Topics

BeginThrottlingCallListBLFSubscriptions, on page 20
CallProcessingNodeCpuPegging, on page 21
CDRAgentSendFileFailed, on page 24
CDRFileDeliveryFailed, on page 24
CDRHighWaterMarkExceeded, on page 25
CDRMaximumDiskSpaceExceeded, on page 25
CodeYellow, on page 30
DBChangeNotifyFailure
DBReplicationFailure
DDRBlockPrevention, on page 31
DDRDown, on page 31
ExcessiveVoiceQualityReports, on page 33
IMEDistributedCacheInactive, on page 34
IMEOverQuota, on page 37
IMEQualityAlert, on page 38
InsufficientFallbackIdentifiers, on page 39
IMEServiceStatus, on page 40
InvalidCredentials, on page 41
LowCallManagerHeartbeatRate
LowTFTPServerHeartbeatRate
MaliciousCallTrace, on page 42
MediaListExhausted, on page 43
MgcpDChannelOutOfService, on page 44
NumberOfRegisteredDevicesExceeded, on page 44
NumberOfRegisteredGatewaysDecreased, on page 45
NumberOfRegisteredGatewaysIncreased, on page 46
NumberOfRegisteredMediaDevicesDecreased, on page 46
NumberOfRegisteredMediaDevicesIncreased, on page 47

NumberOfRegisteredPhonesDropped, on page 47
RouteListExhausted, on page 52
SDLLinkOutOfService, on page 53
TCPSetupToIMEFailed, on page 54
TLSConnectionToIMEFailed, on page 54

BeginThrottlingCallListBLFSubscriptions

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

Table 3: Default Configuration for the BeginThrottlingCallListBLFSubscriptions RTMT Alert

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

CallAttemptBlockedByPolicy

Table 4: Configuration for the CallAttemptBlockedByPolicy Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning

Value	Default Configuration
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 alert every 30 minutes
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

CallProcessingNodeCpuPegging

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

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

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

Table 5: 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

Value	Default Configuration
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

CARIDSEngineCritical

Table 6: Configuration for the CARIDSEngineCritical 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 E-mail	Selected
Trigger Alert Action	Default

CARIDSEngineFailure

Table 7: Configuration for the CARIDSEngineFailure 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: CARIDSEngineFailure event generated.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

CARSchedulerJobFailed

Table 8: Configuration for the CARSchedulerJobFailed 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 E-mail	Selected
Trigger Alert Action	Default

CDRAgentSendFileFailed

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

Table 9: Default Configuration for the CDRAgentSendFileFailed 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: CDRAgentSendFileFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

CDRFileDeliveryFailed

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

Table 10: 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

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable E-mail	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.

Table 11: Default Configuration for the CDRHighWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRHighWaterMarkExceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable E-mail	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 undeliverable files got deleted.

Table 12: 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 E-mail	Selected
Trigger Alert Action	Default

CiscoElmNotConnected

Table 13: Configuration for the CiscoElmNotConnected 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: CiscoElmNotConnected event generated.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Value	Default Configuration
Enable E-mail	Selected
Trigger Alert Action	Default

CiscoGraceTimeLeft

Table 14: Configuration for the CiscoGraceTimeLeft Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CiscoGraceTimeLeft event generated.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

CiscoNoProvisionTimeout

Table 15: Configuration for the CiscoNoProvisionTimeout 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: CiscoNoProvisionTimeout event generated.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

CiscoSystemInDemo

Table 16: Configuration for the CiscoSystemInDemo 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: CiscoSystemInDemo event generated.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

CiscoSystemInOverage

Table 17: Configuration for the CiscoSystemInOverage 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: CiscoSystemInOverage event generated.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

CiscoSystemSecurityMismatch

Table 18: Configuration for the CiscoSystemSecurityMismatch 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: CiscoSystemSecurityMismatch event generated.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

Value	Default Configuration
Schedule	24 hours daily
Enable E-mail	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.

Table 19: Default Configuration for the CodeYellow RTMT Alert

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

Table 20: 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 E-mail	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.

Table 21: Default Configuration for the DDRDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected

Value	Default Configuration
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 E-mail	Selected
Trigger Alert Action	Default

EMCCFailedInLocalCluster

Table 22: Configuration for the EMCCFailedInLocalCluster 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: EMCCFailedInLocalCluster event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alert every 30 minutes
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

EMCCFailedInRemoteCluster

Table 23: Configuration for the EMCCFailedInRemoteCluster 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 alert every 30 minutes
Schedule	24 hours daily
Enable E-mail	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.

Table 24: 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

Value	Default Configuration
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 E-mail	Selected
Trigger Alert Action	Default

IMEDistributedCacheInactive

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

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

Default Configuration

Table 25: Default Configuration for the IMEDistributedCacheInactive 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: Inactive IME Distributed Cache
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable E-mail	Selected

Value	Default Configuration
Trigger Alert Action	Default

ILSHubClusterUnreachable

Table 26: Configuration for the ILSHubClusterUnreachable 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 E-mail	Selected
Trigger Alert Action	Default

ILSPwdAuthenticationFailed

Table 27: Configuration for the ILSPwdAuthenticationFailed Alert

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

Value	Default Configuration
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 E-mail	Selected
Trigger Alert Action	Default

ILSTLSAuthenticationFailed

Table 28: Configuration for the ILSTLSAuthenticationFailed 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
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

IMEDistributedCacheInactive

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

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

Default Configuration

Table 29: Default Configuration for the IMEDistributedCacheInactive 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: Inactive IME Distributed Cache
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

IMEOverQuota

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

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

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

Default Configuration

Table 30: 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 E-mail	Selected
Trigger Alert Action	Default

IMEQualityAlert

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

A large number of the currently active Cisco IME calls have all requested fallback or have fallen back to the PSTN.

A large number of the recent call attempts have gone to the PSTN and not been made over IP.

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

Default Configuration

Table 31: 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 E-mail	Selected
Trigger Alert Action	Default

InsufficientFallbackIdentifiers

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

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

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

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

Default Configuration

Table 32: Default Configuration for the InsufficientFallbackIdentifiers Alert

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

IMEServiceStatus

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

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

Default Configuration

Table 33: Default Configuration for the IMEServiceStatus Alert

Value	Default Configuration
Enable Alert	Selected

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

InvalidCredentials

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

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

Default Configuration

Table 34: 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

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

LocationOutOfResource

Table 35: 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.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

MaliciousCallTrace

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

Table 36: Default Configuration for the MaliciousCallTrace RTMT Alert

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

Table 37: 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

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

MgcpDChannelOutOfService

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

Table 38: 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 D-Channel is out-of-service
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

NumberOfRegisteredDevicesExceeded

This alert occurs when the NumberOfRegisteredDevicesExceeded event gets generated.

Table 39: 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
Enable E-mail	Selected
Trigger Alert Action	Default

NumberOfRegisteredGatewaysDecreased

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

Table 40: 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

Value	Default Configuration
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

NumberOfRegisteredGatewaysIncreased

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

Table 41: Default Configuration for the NumberOfRegisteredGatewaysIncreased RTMT Alert

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

NumberOfRegisteredMediaDevicesDecreased

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

Table 42: Default Configuration for the NumberOfRegisteredMediaDevicesDecreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

Value	Default Configuration
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 E-mail	Selected
Trigger Alert Action	Default

NumberOfRegisteredMediaDevicesIncreased

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

Table 43: 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 E-mail	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.

Table 44: 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 E-mail	Selected
Trigger Alert Action	Default

RecordingCallSetupFail

Table 45: Configuration for the RecordingCallSetupFail 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 alert every 30 minutes
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

RecordingGatewayRegistrationTimeout

Table 46: Configuration for the RecordingGatewayRegistrationTimeout 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 alert every 30 minutes
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

RecordingGatewayRegistrationRejected

Table 47: Configuration for the RecordingGatewayRegistrationRejected 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 alert every 30 minutes

Value	Default Configuration
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

RecordingGatewaySessionFailed

Table 48: Configuration for the RecordingGatewaySessionFailed 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: RecordingGatewaySessionFailed event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alert every 30 minutes
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

RecordingSessionTerminatedUnexpectedly

Table 49: Configuration for the RecordingCallSetupFail 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: RecordingCallSetupFail event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alert every 30 minutes
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

RecordingResourcesNotAvailable

Table 50: Configuration for the RecordingResourcesNotAvailable 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 alert every 30 minutes
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

RouteListExhausted

An available route could not be found in the indicated route list.

Table 51: Default Configuration for the RouteListExhausted RTMT Alert

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

RTMTSessionsExceedsThreshold

Table 52: Configuration for the RTMTSessionsExceedsThreshold 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

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

SDLLinkOutOfService

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

Table 53: 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 E-mail	Selected
Trigger Alert Action	Default

TCPSetupToIMEFailed

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

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

Default Configuration

Table 54: 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 E-mail	Selected
Trigger Alert Action	Default

TLSConnectionToIMEFailed

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

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

Default Configuration

Table 55: Default Configuration for the TLSConnectionToIMEFailed Alert

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

UserInputFailure

Table 56: Configuration for the UserInputFailure 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 alert every 30 minutes

Value	Default Configuration
Schedule	24 hours daily
Enable E-mail	Selected
Trigger Alert Action	Default

Emergency-Level Alarms

The emergency-level alarm equals zero (0) and means that your system or service is unusable. These alarms generally indicate platform failures. Examples follow:

- Service repeatedly fails to startup
- System ran out of disk space while disk space is essential for this system to operate
- System ran out of memory
- Motherboard failure occurred

This level is not suitable for events associated with an individual end point.

BDINotStarted

BDI application not started because of an error.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Emergency (0)

Parameters

Reason [String]

Recommended Action

See application logs for error.

CallDirectorCreationError

There was an error during the CallDirector creation.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Emergency (0)

Parameters

None

Recommended Action

None

CiscoDirSyncStartFailure

Cisco DirSymc application failed to start successfully. Error occurred while starting application

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Emergency (0)

Recommended Action

See application logs for error, may require restarting the application.

ExcceptionInInitSDIConfiguration

Exception occured in InitSDIConfiguration function.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Emergency (0)

Parameters

None

Recommended Action

None

FileWriteError

Cannot write into a file. Failed to write into the primary file path.

Cisco Unified Serviceability Alarm Definition Catalog

System/Generic

Severity

Emergency (0)

Parameters

Primary File Path(String)

Recommended Action

Ensure that the primary file path is valid and the corresponding drive has sufficient disk space. Also, make sure that the path has security permissions similar to default log file path.

GlobalSPUtilsCreationError

There was an error during the GlobalSPUtils creation.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Emergency (0)

Parameters

None

Recommended Action

None

HuntGroupControllerCreationError

There was an error during the HuntGroupController creation.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Emergency (0)

Parameters

None

Recommended Action

None

HuntGroupCreationError

There was an error during the Hunt Group creation.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Emergency (0)

Parameters

None

Recommended Action

None

IPAddressResolveError

The host IP address was not resolved.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Emergency (0)

Parameters

HostName [String]

Recommended Action

None

IPMANotStarted

IPMA application not started because of an error.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Emergency (0)

Parameters

Servlet Name [String] Reason [String]

Recommended Action

See application logs for error.

LineStateSrvEngCreationError

There was an error during the LineStateSrvEng creation.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Emergency (0)

Parameters

None

Recommended Action

None

LostConnectionToCM

TCD connection to CallManager was lost.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Emergency (0)

Parameters

None

Recommended Action

None

NoCMEntriesInDB

There are no CallManager entries in the database.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Emergency (0)

Parameters

None

Recommended Action

None

NoFeatureLicense

No feature license found. Cisco Unified Communications Manager (Unified CM) requires a license to function. Also, Unified CM licenses are version-specific so be certain that the license is for the version you are trying to run. You can run a license unit report in Cisco Unified CM Administration (**System** > **Licensing** > **License Unit Report**).

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Emergency.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Emergency

Recommended Action

Request license generation for Cisco Unified Communications Manager SW FEATURE for your version of Unified CM and upload the license in Cisco Unified CM Administration (**System** > **Licensing** > **License File Upload**).

OutOfMemory

The process has requested memory from the operating system, and there was not enough memory available.

Cisco Unified Serviceability Alarm Definition Catalog

System/Generic

Severity

Emergency (0)

Parameters

None

Recommended Action

None

ServiceNotInstalled

An executable is trying to start but cannot because it is not configured as a service in the service control manager. The service is %s. Service is not installed.

Cisco Unified Serviceability Alarm Definition Catalog

System/Generic

Severity

Emergency (0)

Parameters

Service (String)

Recommended Action

Reinstall the service.

SyncDBCreationError

There was an error during the SyncDB creation in SysController.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Emergency (0)

Parameters

None

Recommended Action

None

SysControllerCreationError

There was an error during the SysController creation.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Emergency (0)

Parameters

None

Recommended Action

None

TapiLinesTableCreationError

There was an error during the TapiLinesTable creation.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Emergency (0)

Parameters

None

Recommended Action

None

TimerServicesCreationError

There was an error during the TimerServices creation.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Emergency (0)

Parameters

None

Recommended Action

None

TestAlarmEmergency

Testing emergency alarm.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Test

Severity

Emergency (0)

Recommended Action

None

WDNotStarted

Failed to startup WebDialer application because of an error.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Emergency (0)

Parameters

Servlet Name [String] Reason [String]

Recommended Action

See application logs for error.

Alert-Level Alarms

The alert-level alarm equals 1 and action must take place immediately. A system error occurred and will not recover without manual intervention. Examples follow:

- Application is about to run out of licenses
- Application is about to run out of disk space
- Application is almost out of memory
- 100% CPU occurs for long period of time

Be aware that this level is not suitable for events that are associated with an individual end point.

CertValidLessthanADay

Certificate is about to expire in less than 24 hours or has expired.

Cisco Unified Serviceability Alarm Definition Catalog

System/CertMonitorAlarmCatalog

Severity

Alert(1)

Routing List

Event Log

Sys Log

Parameters

Message(String)

Recommended Action

Regenerate the certificate that is about to expire by accessing the Cisco Unified Operating System and go to Certificate Management. If the certificate is issued by a CA, generate a CSR, submit the CSR to CA, obtain a fresh certificate from CA, and upload it to Cisco Unified CM.

CMIException

Error while reading the database.

This alarm is always associated with other alarms, which are triggered due to configuring CMI service parameter with invalid values or due to invalid handle value returned by the serial port.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCMIException.

Cisco Unified Serviceability Alarm Definition Catalog

CMIAlarmCatalog/CMI

Severity

ALERT

Routing List

Event Log

SDI

Parameter(s)

CMI Exception(String)

Recommended Action

Refer to the associated alarm for further information.

CMOverallInitTimeExceeded

Initialization of the Cisco Unified Communications Manager system has taken longer than allowed by the value specified in the System Initialization Timer service parameter; as a result, the system will automatically restart now to attempt initialization again. Initialization may have failed due a database error, or due to a large amount of new devices added to the system, or any number of other potential causes. The required time to initialize Cisco Unified Communications Manager has exceeded the time allowed by the Cisco CallManager service parameter, System Initialization Timer. This could be due to an increase in system size.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Name changed from CUCMOverallInitTimeExceeded. • Severity changed from Error to Alert.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Alert

Parameters

Cisco Unified Communications Manager Overall Initialization Time (in minutes) [Int]

Recommended Action

Try increasing the value of the Cisco CallManager service parameter, System Initialization Timer, in the Service Parameters Configuration window in Cisco Unified CM Administration. Use RTMT to discover the number of devices and number of users in the system and evaluate whether the numbers seem accurate. Try increasing the value of the Cisco CallManager service parameter, System Initialization Timer, in the Service Parameters Configuration window in Cisco Unified CM Administration. If increasing the time in the System Initialization Timer service parameter does not correct this issue, contact the Cisco Technical Assistance Center (TAC).

ConfigThreadChangeNotifyServerInstanceFailed

Failed to allocate resources to handle configuration change notification from database. This usually indicates a lack of memory when there is a system issue such as running out of resources.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kConfigThreadChangeNotifyServerInstanceFailed
8.0(1)	Severity changed from Error to Alert.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Alert

Recommended Action

Use RTMT to monitor the system memory resources and consumption and correct any system issues that might be contributing to a reduced amount of system resources.

ConfigThreadChangeNotifyServerSingleFailed

Failed to allocate resources to handle configuration change notification from database. This usually indicates a lack of memory when there is a system issue such as running out of resources.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kConfigThreadChangeNotifyServerSingleFailed.
8.0(1)	Severity changed from Error to Alert.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Alert

Recommended Action

Use RTMT to monitor the system memory resources and consumption and correct any system issues that might be contributing to a reduced amount of system resources.

ConfigThreadChangeNotifyServerStartFailed

Failed to start listening to configuration change notification from database. This usually indicates a lack of memory when there is a system issue such as running out of resources.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kConfigThreadChangeNotifyServerStartFailed.
8.0(1)	Severity changed from Error to Alert.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

ALERT

Recommended Action

Use RTMT to monitor the system memory resources and consumption and correct any system issues that might be contributing to a reduced amount of system resources.

CiscoLicenseApproachingLimit

License units consumption approaching its authorized limit.

Facility/Sub-Facility

CCM_JAVA_APPS_TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Alert (1)

Parameters

Reason [String]

Recommended Action

None

CiscoLicenseOverDraft

Overdraft licenses in use.

Facility/Sub-Facility

CCM_JAVA_APPS_TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Alert (1)

Parameters

Reason [String]

Recommended Action

None

CMVersionMismatch

One or more Unified CM nodes in a cluster are running different Cisco CallManager versions.

This alarm indicates that the local Unified CM is unable to establish communication with the remote Unified CM due to a software version mismatch. This is generally a normal occurrence when you are upgrading a Unified CM node.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ALERT

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameter(s)

Remote Application Link Protocol Version(String)

Local Application Link Protocol Version(String)

Remote Node ID(UInt)

Remote Application ID(Enum)

Remote Application Version(String)

Recommended Action

The alarm details include the versions of the local and remote Unified CM nodes. Compare the versions and upgrade a node if necessary.

Related Topics

Remote Application ID Enum Definitions, on page 72

Remote Application ID Enum Definitions

Value	Definition
100	CallManager
200	CTIManager

CreateThreadFailed

Failed to create a new thread. See Reason string for where it failed. This usually happens when there are system issues such as running out of memory resources.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kCreateThreadFailed.
8.0(1)	Severity changed from Error to Alert.

Facility/Sub-Facility

CCM_TFTP/TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Alert

Parameters

Error [Int] Reason [String]

Recommended Action

Use RTMT to monitor the system memory resources and consumption and correct any system issues that might be contributing to a reduced amount of system resources.

DBLException

An error occurred while performing database activities. A severe database layer interface error occurred. Possible causes for this include the database being unreachable or down or a DNS error.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Alert.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Alert

Parameters

ErrorCode [Int] ExceptionString [String]

Recommended Action

Review the System Reports provided in the Cisco Unified Reporting tool, specifically the Cisco Unified CM Database Status report, for any anomalous activity. Check network connectivity to the server that is running the database. If your system uses DNS, check the DNS configuration for any errors.

InvalidCredentials

Credential Failure to IME server.

The connection to the IME server could not be completed, because the username and/or password configured on Unified CM do not match those configured on the IME server.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	New Alarm for this release.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ALERT

Recommended Action

The alarm will include the username and password which were used to connect to the IME server, along with the IP address of the target IME server and its name. Log into the IME server and check that the username and password configured there match those configured in Unified CM.

Routing List

SDL

SDI

Sys Log

Event Log

Alert Manager

Parameter(s)

User name(String)

IP address(String)

Server name(String)

MemAllocFailed

Memory allocation failed.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kMemAllocFailed. Severity changed to Alert. Recommended action changed.

Facility/Sub-Facility

CCM_SUMI-CMI

Cisco Unified Serviceability Alarm Definition Catalog

System/Service Manager

Severity

Alert

Parameters

Memory Allocation Failure(String)

Recommended Action

1. Check the syslog for the system error number.
2. If the Alert is seen repeatedly, restart Service Manager.
3. If the problem still persist, reboot the Cisco Unified CM node.

NoDbConnectionAvailable

No database connection available. Database layer could not find any working database connection.

Facility/Sub-Facility

CCM_DB_LAYER-DB

Cisco Unified Serviceability Alarm Definition Catalog

System/DB

Severity

Alert (1)

Recommended Action

In Cisco Unified Serviceability, enable Detailed level traces in the Trace Configuration window for the Cisco Database Layer Monitor service. Check network connectivity and operation of SQL Server services.

ParityConfigurationError

The CMI service parameter, Parity, has an invalid configuration.

An invalid parity has been configured for the serial port that CMI uses to connect to the voice messaging system. It is possible that the parity value has been updated via AXL or a CLI command where validation of the value was not performed. For this reason, it is best to set this value in the Service Parameter Configuration window in Cisco Unified CM Administration and the value can be validated against the accepted range of values for this field.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	New name changed from kParityConfigurationError.

Cisco Unified Serviceability Alarm Definition Catalog

CMIAlarmCatalog/CMI

Severity

ALERT

Routing List

Event Log

SDI

Parameter(s)

Illegal Parity(String)

Recommended Action

Verify that the Cisco Messaging Interface service parameter Parity is set to a valid (allowable) value.

SerialPortOpeningError

When CMI tries to open the serial port, the operating system returns an error.

For a system running CMI, the serial port through which the voice messaging system is connected is always USB0, and that value is configured in the Cisco Messaging Interface service parameter, Serial Port. It is possible that the Serial Port value has been updated via AXL or a CLI command where validation of the value was not performed. CMI triggers this alarm if the value in the Serial Port service parameter is anything other than USB0.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	New name changed from kSerialPortOpeningError.

Cisco Unified Serviceability Alarm Definition Catalog

CMIAlarmCatalog/CMI

Severity

ALERT

Routing List

Event Log

SDI

Parameter(s)

Serial Port Opening Error(String)

Recommended Action

Ensure that USB0 is configured in the Cisco Messaging Interface service parameter Serial Port. Also, physically confirm that the cable is firmly connected to the USB0 port.

SDIControlLayerFailed

Failed to update trace logging or alarm subsystem for new settings. This usually indicates a lack of system resources or a failure in database access by the trace logging or alarm subsystem.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Critical to Alert.
7.0(1)	Name changed from kSDIControlLayerFailed.

Facility/Sub-Facility

CCM_TFTP_TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Alert

Parameters

Error [Int] Reason [String]

Recommended Action

In Cisco Unified Serviceability, enable Detailed level traces in the Trace Configuration window for TFTP and Cisco Database Layer Monitor services. Also, use RTMT to look for errors that may have occurred around the time of the alarm. Ensure that the database server is running, and that the Cisco Database Layer Monitor service is running without problems. If this alarm persists, contact the Cisco Technical Assistance Center (TAC) with TFTP service and database trace files.

SDLLinkOOS

SDL link to remote application out of service. This alarm indicates that the local Unified CM has lost communication with the remote Unified CM. This alarm usually indicates that a node has gone out of service (whether intentionally for maintenance or to install a new load for example; or unintentionally due to a service failure or connectivity failure).

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Alert.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Alert

Parameters

Remote IP address of remote application [String] Unique Link ID. [String] Local node ID [UInt] Local Application ID. [Enum]RemoteNodeID [UInt] Remote application ID. [Enum]

Recommended Action

In the Cisco Unified Reporting tool, run a CM Cluster Overview report and check to see if all servers can talk to the Publisher. Also check for any alarms that might have indicated a CallManager failure and take appropriate action for the indicated failure. If the node was taken out of service intentionally, bring the node back into service.

Related Topics

LocalApplicationID and RemoteApplicationID Enum Definitions, on page 79

LocalApplicationID and RemoteApplicationID Enum Definitions

Code	Reason
100	CallManager
200	CTI

SocketError

Failed to open network connection for receiving file requests. This usually happens when the IP address that the TFTP service uses to open the network connection is invalid.

Table 57: History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kSocketError.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Alert (1)

Parameters

Error [Int] Reason [String]

Recommended Action

Verify that the TFTP service parameter, TFTP IP Address, accurately specifies the IP address of the NIC card to use for serving files via TFTP. See the help for the (advanced) TFTP IP Address service parameter for more information. If the problem persists, go to Cisco Unified Serviceability and enable Detailed level traces in the Trace Configuration window for the TFTP service and contact the Cisco Technical Assistance Center (TAC).

StopBitConfigurationError

The Cisco Messaging Interface service parameter, Stop Bits, has an invalid configuration.

An invalid stop bit has been configured for the serial port that CMI uses to connect to the voice messaging system. It is possible that the Stop Bits value has been updated via AXL or a CLI command where validation of the value was not performed. For this reason, it is best to set this value in the Service Parameter Configuration window in Cisco Unified CM Administration and the value can be validated against the accepted range of values for this field.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	New name changed from kStopBitConfigurationError.

Cisco Unified Serviceability Alarm Definition Catalog

CMIAlarmCatalog/CMI

Severity

ALERT

Routing List

Event Log

SDI

Parameter(s)

Illegal Stop Bit(String)

Recommended Action

Verify that the Cisco Messaging Interface service parameter Stop Bits is set to a valid (allowable) value.

TFTPServerListenSetSockOptFailed

Failed to increase the size of the network buffer for receiving file requests. This usually indicates a lack of memory when there is a system issue such as running out of resources.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kTFTPServerListenSetSockOptFailed.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Alert (1)

Parameters

Error [Int] IPAddress [String] Port [Int]

Recommended Action

Use RTMT to monitor the system memory resources and consumption and correct any system issues that might be contributing to a reduced amount of system resources.

TFTPServerListenBindFailed

Fail to connect to the network port through which file requests are received. This usually happens if the network port is being used by other applications on the system or if the port was not closed properly in the last execution of TFTP server.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kTFTPServerListenBindFailed.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Alert (1)

Parameters

Error [Int] IPAddress [String] Port [Int]

Recommended Action

Verify that the port is not in use by other application. After stopping the TFTP server, at the command line interface (CLI) on the TFTP server, execute the following command—show network status listen. If the port number specified in this alarm is shown in this CLI command output, the port is being used. Restart the Cisco Unified Communications Manager system, which may help to release the port. If the problem persists, go to Cisco Unified Serviceability and enable Detailed level traces in the Trace configuration window for the TFTP service and contact the Cisco Technical Assistance Center (TAC).

TestAlarmAlert

Testing alert alarm.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Test

Severity

Alert (1)

Recommended Action

None

TLSConnectionToIMEFailed

TLS Failure to IME service.

A TLS connection to the IME server could not be established because of a problem with the certificate presented by the IME server. (For example, not in the Unified CM CTL, or is in the CTL but has expired).

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	New Alarm for this release.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ALERT

Recommended Action

Check to see that the certificate of the IME server is configured properly in the Unified CM.

Routing List

SDL

SDI

Sys Log

Event Log

Alert Manager

Parameter(s)

SSLErrorCode(UInt)

SSLErrorText(String)

TVSServerListenBindFailed

Fail to connect to the network port through which file requests are received. This usually happens if the network port is being used by other applications on the system or if the port was not closed properly in the last execution of TVS server.

Cisco Unified Serviceability Alarm Catalog

System/TVS

Severity

ALERT

Routing List

SDI

Event Log

Data Collector

Sys Log

Parameter(s)

nError(Int)

IPAddress(String)

Port(Int)

Recommended Action

Verify that the port is not in use by other application. After stopping the TVS server, at the command line interface (CLI) on the TVS server, execute the following command: show network status listen. If the port number specified in this alarm is shown in this CLI command output, the port is being used. Restart the Cisco Unified Communications Manager system, which may help to release the port. If the problem persists, go to Cisco Unified Serviceability and enable Detailed level traces in the Trace Configuration window for the TVS service and contact the Cisco Technical Assistance Center (TAC).

TVSServerListenSetSockOptFailed

Failed to increase the size of the network buffer for receiving file requests. This usually indicates a lack of memory when there is a system issue such as running out of resources.

Cisco Unified Serviceability Alarm Catalog

System/TVS

Severity

ALERT

Routing List

SDI

Event Log

Data Collector

Sys Log

Parameter(s)

nError(Int)

IPAddress(String)

Port(Int)

Recommended Action

Use RTMT to monitor the system memory resources and consumption and correct any system issues that might be contributing to a reduced amount of system resources.

UnknownException

Unknown error while connecting to database.

When CMI service is started, it tries to read CMI service parameters from DB. During this, if there is an unknown error, CMI triggers this alarm.

Cisco Unified Serviceability Alarm Definition Catalog

CMIAlarmCatalog/CMI

Severity

ALERT

Routing List

Event Log

SDI

Recommended Action

Report to Customer Service representative.

VMDNConfigurationError

The Voice Mail DN for CMI is invalid.

CMI cannot register with Cisco Unified Communications Manager because of an invalid Voice Mail DN. This alarm occurs because the Cisco Messaging Interface service parameter, Voice Mail DN, is empty or has invalid characters other than digits (0-9). It is possible that the Voice Mail DN value has been updated via AXL or a CLI command where validation of the value was not performed. For this reason, it is best to set this value in the Service Parameter Configuration window in Cisco Unified CM Administration and the value can be validated against the accepted range of values for this field.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kVMDNConfigurationError.

Cisco Unified Serviceability Alarm Definition Catalog

CMIAlarmCatalog/CMI

Severity

ALERT

Routing List

Event Log

SDI

Parameter(s)

Invalid Voice Mail DN(String)

Recommended Action

Check the CMI service parameter Voice Mail DN to confirm that a valid directory number has been configured.

Critical-Level Alarms

The critical-level alarm equals 2 and action may need to be taken immediately; auto-recovery is expected, but monitor the condition.

This alarm acts similar to the alert-level alarm but not necessarily requiring an immediate action. A system-affecting service had a failure but recovered without intervention. Examples follow:

- Service crashed due to an error that could not be handled but a watchdog process exists that will restart the service. The crash does not necessarily require immediate action. Examples are:
  - Out of memory conditions
  - Uninitialized variables
  - Memory scribblers
- Unexpected code error occurred that could not be handled but for which the system automatically restarts.

BChannelOOS

The B-channel is out of service. The B-channel indicated by this alarm has gone out of service. Some of the more common reasons for a B-channel to go out of service include are as follows:

- Taking the channel out of service intentionally to perform maintenance on either the near- or far-end
- MGCP gateway returns an error code 501 or 510 for a MGCP command sent from Cisco Unified Communications Manager (Cisco Unified CM)
- MGCP gateway does not respond to an MGCP command sent by Cisco Unified CM three times
- Speed and duplex mismatch exists on the Ethernet port between Cisco Unified CM and the MGCP gateway.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Changed severity level from Error to Critical.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Critical

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

Unique channel Id [String] Device Name. [String] Reason. [Enum]Channel Id. [UInt]

Enum Definitions

- 0—None Defined

Recommended Action

Check the Cisco Unified CM advanced service parameter, Change B-channel Maintenance Status to determine if the B-channel has been taken out of service intentionally; Check the Q.931 trace for PRI SERVICE message to determine whether a PSTN provider has taken the B-channel out of service; Reset the MGCP gateway; Check the speed and duplex settings on the Ethernet port.

CallManagerFailure

Indicates an internal failure in the Cisco Unified Communications system. The service should restart in an attempt to clear the failure.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Critical.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Critical

Parameters

Additional Text [Optional] [String] Host name of hosting node. [String] IP address of hosting node. [String] Reason code. [Enum]

Recommended Action

Monitor for other alarms and restart the Cisco CallManager service, if necessary. Collect the existing trace files in case the alarm persists.

CISCO-CCM-MIB

Part of ccmCallManagerAlarmEnable. See CISCO-CCM-MIB for more information.

Related Topics

Reason Code Enum Definitions for CallManagerFailure, on page 88
CISCO-CCM-MIB

Reason Code Enum Definitions for CallManagerFailure

Code	Reason
1	Unknown—Unified CM has failed for an unknown reason.
2	HeartBeatStopped—An internal heart beat has stopped after the preceding heart beat interval.
3	RouterThreadDied—An internal thread has failed.
4	TimerThreadDied—An internal thread has failed.
5	CriticalThreadDied—An internal thread has failed.

CertExpiryCritical

Certificate is about to expire in less than 7 days. Regenerate or reimport certificate. Name of the service generating this alarm is Cisco Certificate Expiry Monitor. The alarms are generated when any certificate generated by the system or uploaded into the system expires. Cisco Unified CM uses certificates for Tomcat (Web Server), CallManager, IPSEc and Directory. Refer Security guide for more details on various certificates. When a certificate generated by Cisco Unified CM, the default validity of the self-signed certificate is for 5 years. In case of Certificates signed by a CA, the validity is dependent on the Expiry date set by CA while issuing the certificate. Once a certificate is about to expire “Cisco Certificate Expiry Monitor” service generates alarms. The severity of the alarm is dependent on how much time is left for the certificate to expire.

The impact to system operation depends on the which certificate expired. This information is contained in the alarm. If Tomcat certificate expired, while connecting to Cisco Unified CM web pages, browser will throw an error stating certificate has expired. One can still ignore the warning and continue to connect to Cisco Unified CM pages.

In case of Directory-trust, if Directory trust certificate uploaded to Cisco Unified CM expires, Cisco Unified CM may not be able to establish SSL connection with external LDAP server. The overall impact is that SSL connection between Cisco Unified CM and other external Servers will fail.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.

Facility/Sub-Facility

/CERT

Cisco Unified Serviceability Alarm Definition Catalog

System/Cert Monitor

Severity

Critical (2)

Parameters

None

Recommended Action

Login to CUOS page. Go to **Security** > **Certificate Management** and regenerate the certificate that has expired (based on the information in alarm). This will generate a new self-signed certificate with a new expiry date. In case the certificate is signed by a CA, Generate a new CSR, send it to the CA, get the certificate signed by CA and upload the new certificate.

CertValidfor7days

Alarm indicates that the certificate has expired or expires in less than seven days.

Cisco Unified Serviceability Alarm Definition Catalog

System/CertMonitorAlarmCatalog

Severity

Critical(2)

Routing List

Event Log

Sys Log

Parameters

Message(String)

Recommended Action

Regenerate the certificate that is about to expire by accessing the Cisco Unified Operating System and go to Certificate Management. If the certificate is issued by a CA, generate a CSR, submit the CSR to CA, obtain a fresh certificate from CA, and upload it to Cisco Unified CM.

CDRMaximumDiskSpaceExceeded

The CDR files disk usage exceeded maximum disk allocation. Some undeliverable files may have been deleted to bring disk usage down. The CDR files disk usage has exceeded the maximum allocated disk space. CDRM may have deleted some CDR files that have not been sent to the outside billing servers yet, in order to bring the disk usage down to below High Water Mark. The decision whether to delete undeliverable files or not depends on how deletionDisable flag is configured at CDRM Configuration page. E-mail alert will be sent to the admin.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Facility and sub-facility changed. Added Routing List and changed Data Collector to Alert Manager.

Facility/Sub-Facility

CDRREP

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CDR Management

Severity

Critical (2)

Routing List

Event Log

Sys Log

Alert Manager

Parameters

DiskUsageInMB [String]

Recommended Action

1. Check if there are too many undeliverable CDR files accumulated due to some condition.
2. Check network link status.
3. Check if billing server is alive.
4. Check if (s)FTP Server on the billing server is running and accepting request.
5. Check if CDRM Configuration for billing servers is correct - under **Serviceability** > **Tools**.
6. Check if CDR files maximum disk allocation is too low - under **Serviceability** > **Tools**.
7. Check CDR Repository Manager trace under `/var/log/active/cm/trace/cdrrep/log4j`.

CiscoDirSyncProcessFailToStart

LDAPSync process failed to start on particular sync agreement.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Critical (2)

Parameters

AgreementId [String]

Recommended Action

See application logs for error

CodeRedEntry

Unified CM has entered Code Red condition and will restart.

Unified CM has been in Code Yellow state for an extended period and is unlikely to recover on its own. The Cisco CallManager service automatically restarts in an attempt to clear the condition that is causing the Code Yellow state. The amount of time that the system will remain in Code Yellow state is configurable in the Code Yellow Duration service parameter. If the duration of this parameter is set to 99999, Code Red condition will never occur.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Critical.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Critical

Parameters

Expected Average Delay [UInt] Entry Latency [UInt] Exit Latency [UInt] Sample Size [UInt] Code Yellow Duration [UInt] Number of Calls Rejected Due to Call Throttling [UInt] Total Code Yellow Entry [UInt] Total Code Yellow Exit [UInt]

Recommended Action

You should have attempted the steps in the recommended actions defined in the CodeYellowEntry alarm. If you have not, try those after the system is online. There is no other action for Code Red because the only action is to restart which is performed for you automatically.

CodeYellowEntry

CallManager has initiated call throttling due to unacceptably high delay in handling incoming calls.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Critical.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Critical

Parameters

Expected Average Delay [UInt] Entry Latency [UInt] Exit Latency [UInt] Sample Size [UInt] Total Code Yellow Entry [UInt]

Recommended Action

Memory problems or high CPU usage are generally at the root of a Code Yellow state. A bad disk could also be the cause. Also, trace level settings can consume tremendous amounts of CPU (especially when the Enable SDL TCP Event Trace checkbox is enabled on the SDL Trace Configuration window in Cisco Unified Serviceability). Check these areas to try to correct the Code Yellow condition. You can also determine the level of fragmentation on the hard disk by issuing the File Fragmentation command from the CLI for the trace directories. Monitor the situation and collect existing trace files. If the CodeYellowExit alarm is not issued in a reasonable amount of time as deemed by your organization, or if the system is frequently entering Code Yellow state, contact TAC and supply the trace information you have collected.

CoreDumpFileFound

The new core dump files have been found in the system. One of the component has crashed and generated a core dump. Use admin cli or RTMT to featch the backtrace.

Facility/Sub-Facility

CCM_TCT-LPMTCT

Cisco Unified Serviceability Alarm Definition Catalog

System/LpmTct

Severity

Critical (2)

Parameters

TotalCoresFound [String] CoreDetails [String] Core1 [String] Core2 [String] Core3 [String] Core4 [String] Core5 [String] Core6 [String]

Recommended Action

This serious internal error should be investigated by the Cisco Technical Assistance Center (TAC). Before contacting TAC, Login to cli on CCM serve and run “active analyze core file name” to generate the backtrace of the core dump. The core file name is listed in the alert details. After the analyze command is executed, collect the backtrace using cli command “file get activelog analyze” or “Collect Traces” option from RTMT. Send these backtraces to Cisco TAC for further analysis.

DChannelOOS

The D-channel is out of service. D-channel indicated by this alarm has gone out of service. Common reasons for a D-channel going out of service include losing T1/E1/BRI cable connectivity; losing the gateway data link (Layer 2) due to an internal or external problem; or gateway reset.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Critical.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Critical

Parameters

Channel Id. [UInt] Unique channel Id [String] Device Name. [String] Device IP address [String] Reason. [Enum]

Enum Definitions

- 0—None Defined

Recommended Action

Check the connection of the T1/E1/BRI cable; reset the gateway to restore Layer 2 connectivity; investigate whether the gateway reset was intentional. If the reset was not intentional, take steps to restrict access to the Gateway Configuration window in Cisco Unified CM Administration and the gateway terminal.

DUPLEX_MISMATCH

This alarm is generated by Cisco CDP whenever there is a duplex mismatch between local interface and switch interface.

Cisco Unified CommunicationsRelease	Action
7.1	Added DUPLEX_MISMATCH to the CDPAlarmCatalog.

Facility/Sub-Facility

CCM_CDP/CDP

Cisco Unified Serviceability Alarm Definition Catalog

System/CDP

Severity

Critical (2)

Parameters

Switch Duplex Settings(String)

Local Interface Duplex Settings(String)

Recommended Action

Ensure that duplex settings are set to auto or full on local interface as well as switch interface.

ErrorChangeNotifyClientBlock

A change notification client is busy (blocked). If the change notification client continues to be blocked for 10 minutes, the system automatically clears the block and change notification should resume successfully. Changes made to the database are not being consumed by one of the recipients. This does not always represent an issue. However, if the change notification client continues to be blocked for 10 minutes, the system automatically clears the block for all clients except the blocked one, which means that change notifications should resume successfully for all other clients. To clear the blocked client, you must restart the server.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Changed severity level to Critical from Error.

Facility/Sub-Facility

CCM_DB_LAYER-DB

Cisco Unified Serviceability Alarm Definition Catalog

System/DB

Severity

Critical (2)

Recommended Action

At the command line interface (CLI) on the database server, execute the following command:

show tech notify

The CLI command output will provide information about the block. Use Cisco Unified Serviceability to restart the server that was indicated in the alarm. You may also want to gather traces to examine them for anomalous activity during the time that client was blocked. In Cisco Unified Serviceability, enable Detailed level traces in the Trace Configuration window for the Cisco Database Layer Monitor service. Also, use RTMT to look for a change that may have occurred around the time of the alarm.

LogPartitionHighWaterMarkExceeded

The percentage of used disk space in the log partition has exceeded the configured high water mark. Some of the core file and / or trace files will be purged until the percentage of used disk space in the log partition gets below the configured low water mark.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Critical.

Facility/Sub-Facility

CCM_TCT-LPMTCT

Cisco Unified Serviceability Alarm Definition Catalog

System/LpmTct

Severity

Critical

Parameters

UsedDiskSpace [String] MessageString [Optional]. [String]

Recommended Action

Login into RTMT and check the configured threshold value for LogPartitionHighWaterMarkExceeded alert in Alert Central. If the configured value is set to a lower than the default threshold value unintentionally, change the value to default.

If you continue to receive this alert for half an hour after receiving the 1st alert, check for the disk usage for Common partition under "Disk Usage" tab in RTMT. If the disk usage shown under that tab is higher than configured value in LogPartitionLowWaterMarkExceeded alert configuration, contact Cisco TAC to troubleshoot the cause of high disk usage in Common partition.

MaxCallsReached

The maximum number of simultaneous connections in a Cisco Unified Communications Manager (Unified CM) node has been reached. This is an internally-set value and when it is exceeded, Unified CM starts throttling calls to keep the number of calls below the internal threshold.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Critical.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Critical

Parameters

Description [Int]

Recommended Action

In the Real-Time Monitoring Tool, check the CallsActive counter in the Cisco CallManager object for an unusually high number of calls. Internal mechanisms will attempt to correct this condition. If this alarm continues to occur, collect existing SDL and CCM trace files and check to be sure that CM Services trace collection in Cisco Unified CM Serviceability is set to Detailed level.

MGCPGatewayLostComm

The MGCP gateway is no longer in communication with Cisco Unified Communications Manager (Cisco Unified CM). This could occur because Cisco Unified CM receives an MGCP unregister signal from the

gateway such as RSIP graceful/forced; Cisco Unified CM doesn't receive the MGCP KeepAlive signal from the gateway; the MGCP gateway doesn't response to an MGCP command sent by Cisco Unified CM three times; a speed and duplex mismatch exists on the Ethernet port between Cisco Unified CM and the MGCP gateway; the gateway has reset.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Critical (2)

Parameters

Device Name [String]

Recommended Action

Reset the MGCP gateway in an attempt to restore communication with Cisco Unified CM; check the speed and duplex settings on the Ethernet port. In the case of an unwanted reset of the gateway which caused communication to be lost, take precautions to ensure that no unauthorized personnel resets the gateway from Cisco Unified CM Administration or via the gateway terminal.

Related Topics

CISCO-CCM-MIB

StationTCPInitError

An error during initialization was encountered.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Error to Critical. • Following parameters are removed: ◦ Error Number [String] ◦ ErrorCode [Int]

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Critical

Recommended Action

Verify the Cisco Unified Communications Manager IP address is configured and is not configured as the loop back address for the IP version. If the IP settings are correct, collect SDL and SDI traces and contact TAC.

TCPSetupToIMEFailed

Connection Failure to IME server.

This alarm occurs when Unified CM is unable to establish a TCP connection to an IME server. It typically occurs when the IP address and port of the IME server are misconfigured or an Intranet connectivity problem is preventing the connection from being set up.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

CRITICAL_ALARM

Recommended Action

Check to make sure that the IP address and port of the IME server - which are present in the alarm - are valid. If so, this may be due to a network connectivity problem. Test the connectivity between the Unified CM servers and the IME server.

Routing List

SDL

SDI

Sys Log

Event Log

Alert Manager

Parameter(s)

IP address(String)

Port number(UInt)

TimerThreadSlowed

Verification of the Cisco Unified Communications Manager (Unified CM) internal timing mechanism has slowed beyond acceptable limits. This generally indicates an increased load on the system or an internal anomaly.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Warning to Critical.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Critical

Recommended Action

If this alarm occurs at the same general day or time, or if it occurs with increasing frequency, collect all system performance data in Real-Time Monitoring Tool as well as all trace information for the 30 minutes prior to the time that this alarm occurred and contact TAC.

TestAlarmCritical

Testing critical alarm.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Test

Severity

Critical (2)

Recommended Action

None

Error-Level Alarms

The error-level alarm is 3 and you should investigate important devices or subsystems and determine if immediate action is needed. Errors that do not necessarily impact the ability of the service to continue to function and do not create a system outage. More related to device or subsystems.

An example would be a device or subsystem failing for an unexpected reason.

ANNDeviceRecoveryCreateFailed

ANN device recovery create failure. The ANN device recovery class create failed, possibly due to lack of memory. If the error code is non-zero it may help determine the cause of the error. The announcement device will not be available.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
8.0(1)	Added Routing List elements and Parameters.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error (3)

Routing List

SDI

Event Log

Sys Log

Parameters

OS Error Code(Int)

OS Error Description(String)

Recommended Action

Restart the Cisco IP Voice Media Streaming App service or restart server.

AwaitingResponseFromPDPTimeout

Cisco Unified Communication Manager timed out waiting for the routing response from the policy decision point. Cisco Unified Communications Manager (Unified CM) did not receive a call routing response from the policy decision point (PDP) within the time specified by the Cisco CallManager service parameter, Call Intercept Routing Request Timer, or on the Call Intercept Profile Configuration window in Cisco Unified CM Administration.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR_ALARM

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Policy Decision Point(String)

Recommended Action

Check whether the PDP is in service and working normally. Verify that the PDP is not overloaded; if it is, take appropriate action to reduce the load on the PDP by following some or all of these recommendations:

- Consider adding more PDPs and provisioning Unified CM with additional call intercept profiles and call intercept trigger points in the various configuration pages under the Call Routing menu in Cisco Unified CM Administration.
- Provision a pair of policy servers per call-intercept profile to enable load balancing.

  OR

- Verify that the PDP server in your deployment meets or exceed the hardware requirements specified in the documentation for Cisco Enterprise Policy Manager (CEPM) or the third-party PDP solution you have deployed. If necessary, increase the value in the Cisco CallManager service parameter, Call Intercept Routing Request Timer or the value in the Call Intercept Profile for this PDP.

BadCDRFileFound

Bad CDR or CMR flat file found during CDR Load to CAR database. The file could be corrupted. However, CAR loader is able to skip the bad records and load the good ones to CAR database. The name of the service generating this alarm is CAR Loader (DailyCdrLoad) job. Part of Cisco CAR Scheduler service.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Existing parameters added.
7.0(1)	Error message added.

Facility/Sub-Facility

CCM_CAR_SCH-CAR

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CDR Rep

Severity

Error (3)

Parameters

File Name(String)

First Bad Record Cause(String)

File Summary(String)

Recommended Action

Find the bad file from the cdr_repository folders, and check its problematic record based on the information given by the cause and summary. Collect the associated SDI and SDL traces for the bad records found in this file as soon as possible. Collect and check the CAR Scheduler traces for more details.

BDIApplicationError

BDI Facility/Sub-Facility error.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Reason [String]

Recommended Action

See application logs for details

BDIOverloaded

BDI Facility/Sub-Facility overloaded.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Reason [String]

Recommended Action

See application logs for details.

CARSchedulerJobError

CAR scheduled job failed. A normal CAR scheduled job failed such as the pre-generated Daily/Weekly/Monthly/Monthly-Bill reports jobs. The particular CAR scheduler job that fails cannot be run properly. This does not cause any significant impact on CAR functions. For pre-generated CAR report, this would result failure to run on a particular report, which leads to missing of CAR report.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Existing parameters added.
7.0(1)	Error message added.

Facility/Sub-Facility

CCM_CAR_SCH-CAR

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CAR

Severity

Error (3)

Parameters

Job Name(String)

Job Failure Cause(String)

Job Failure Detail(String)

Recommended Action

1. Check the status of Cisco CAR Scheduler service.
2. Check the Event Log from CAR page.
3. Check the contents in tbl_system_preferences table.
4. Check the number of records in tbl_billing_data, tbl_billing_error, and tbl_error_id_map tables.
5. Check if the scheduled job configuration is correct from CAR page.
6. Collect and check the CAR Scheduler traces for more details.

CARSchedulerJobFailed

Critical CAR scheduled job failed. The jobs are PopulateSchedules, DailyCdrLoad, TaskMonitor, or DatabaseMaintenance. The particular CAR scheduler job that failed cannot be run properly. This can cause significant impact on CAR functions.

- If PopulateSchedules job fails, CAR scheduler cannot schedule jobs to run for the day; this would result some/all of CAR scheduler jobs cannot start.
- If DailyCdrLoad job fails, CAR loader would not be able to load CDR/CMR records from CDR/CMR flat files into CAR database; this would result records found upon running CAR reports, and causes accumulation of CDR/CMR flat files unprocessed.
- If TaskMonitor job fails, CAR scheduler will not be able to perform the daily DB IDS memory clean up task; this would result higher DB shared memory usage.
- If DatabaseMaintenance job fails, CAR scheduler will not be able to perform the daily optimized database maintenance Update statistics procedures; this would result CAR database not optimized for its operations.

Name of the service generating this alarm is CAR Scheduler service.

Cisco Unified CommunicationsRelease	Action
8.0(1)	Routing list changed from Data Collector to Alert Manager and existing parameters added.

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.

Facility/Sub-Facility

CAR

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CAR Alarm Catalog

Severity

Error

Routing List

Event Log

Sys Log

Alert manager

Parameters

Job Name(String)

Job Failure Cause(String)

Job Failure Detail(String)

Recommended Action

1. Check the status of Cisco CAR DB service.
2. Check the status of Cisco CAR Scheduler service.
3. Check the Event Log from CAR page.
4. Check the contents in tbl_system_preferences table.
5. Check the number of records in tbl_billing_data, tbl_billing_error, and tbl_error_id_map tables.
6. Check if the scheduled job configuration is correct from CAR page.
7. Collect and check the CAR Scheduler traces for more details.

CCDIPReachableTimeOut

CCD Requesting Service IP Reachable Duration times out.

The CCD requesting service detected that it can no longer reach the learned patterns through IP. All learned patterns from this forward will be marked as unreachable (via IP) and to allow calls to learned patterns to

continue to be routed until IP becomes reachable again, all calls to learned patterns will be routed through the PSTN. Calls can be routed through the PSTN for a certain period of time before PSTN failover times out.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Event Log

Recommended Action

Check IP connectivity and resolve any TCP or IP problems in the network.

CCDPSTNFailOverDurationTimeOut

The internal limit on PSTN failover has expired.

When learned patterns are not reachable through IP, Unified CM routes calls through the PSTN instead. Calls can be routed through PSTN for an internally-controlled duration. When this alarm occurs, the PSTN failover duration has expired and calls to learned patterns cannot be routed. All learned patterns will be purged from Unified CM.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Event Log

Recommended Action

Troubleshoot your network to get IP connectivity restored. After IP connectivity is restored, Unified CM will automatically relearn Hosted DN patterns and calls to learned patterns will proceed through IP.

CDRAgentSendFileFailed

CDR Agent cannot send CDR files from CCM node to CDR Repository node within the CCM cluster because of timeout or other reasons. E-mail alert will be sent to the admin.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Changed Data Collector Routing List element to Alert Manager.

Facility/Sub-Facility

CDRREP

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CDR Rep

Severity

Error (3)

Routing List

Event Log

Sys Log

Alert Manager

Parameters

CDRRepositoryNodeAddress [String]

CDRAgentNodeAddress [String]

Recommended Action

1. Check network link status.
2. Check if CDR Repository node (first node in the cluster) is alive.
3. Check if CDR Repository Manager is activated on the first node.
4. Check CDRM Configuration under **Serviceability** > **Tools**.
5. Check CDR Agent trace on the specific node where error occurred.
6. Check CDR Repository Manager trace.
7. Check if the Publisher is being upgraded. If the CDRAgentSendFileFailureContinues alarm is no longer present, the condition is corrected.

CDRAgentSendFileFailureContinues

CDR Agent cannot send CDR files from CCM node to CDR Repository node on retries. CDR Agent cannot send CDR files on retries after the initial failure from CCM node to CDR Repository node within the cluster.

Facility/Sub-Facility

CCM_CDR_REP-CDRREP

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CDR Rep

Severity

Error

Routing List

Event Log

Sys Log

Data Collector

Parameters

CDRRepositoryNodeAddress [String]

CDRAgentNodeAddress [String]

Recommended Action

1. Check network link status.
2. Check if CDR Repository node (first node in the cluster) is alive.
3. Check if CDR Repository Manager is activated on the first node.
4. Check CDRM Configuration under **Serviceability** > **Tools**.
5. Check CDR Agent trace on the specific node where error occurred.
6. Check CDR Repository Manager trace.
7. Check if the Publisher is being upgraded.

CDRFileDeliveryFailed

FTP delivery of CDR files to the Billing Server outside of the cluster failed because of timeout or other reasons. E-mail alert will be sent to the admin.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Changed Data Collector Routing List element to Alert Manager.

Facility/Sub-Facility

CDRManagement/CDRREP

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CDR Rep

Severity

Error (3)

Routing List

Event Log

Sys Log

Alert Manager

Parameters

BillingServerAddress [String]

Recommended Action

1. Check network link status.
2. Check if billing server is alive.
3. Check if (s)FTP Server on the billing server is running and accepting request.
4. Check if CDRM Configuration is correct under **Serviceability** > **Tools**.
5. Check CDR Repository Manager trace.

CDRFileDeliveryFailureContinues

(s)FTP delivery of CDR files failed on retries to the Billing Server outside of the cluster failed on retries after the initial failure.

Facility/Sub-Facility

CCM_CDR_REP-CDRREP

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CDR Rep

Severity

Error (3)

Routing List

Event Log

Sys Log

Data Collector

Parameters

BillingServerAddress [String]

Recommended Action

1. Check network link status.
2. Check if billing server is alive.
3. Check if (s)FTP Server on the billing server is running and accepting request.
4. Check if CDRM Configuration is correct - under **Serviceability** > **Tools**.
5. Check CDR Repository Manager trace.

CFBDeviceRecoveryCreateFailed

The CFB device startup failed, possibly due to lack of memory. If the error code is non-zero it may help determine the cause of the error. The conference bridge device will not be available.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Added Routing List elements and Parameters.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error (3)

Routing List

SDI

Event Log

Sys Log

Parameter(s)

OS Error Code(Int)

OS Error Description(String)

Recommended Action

Restart the Cisco IP Voice Media Streaming App service or restart server.

CiscoDhcpdFailure

DHCP Daemon stopped running. DHCP Daemon cannot be brought up due to configuration error or crash.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Reason [String]

Recommended Action

Check application log for errors and correct the configuration. May require restarting the application if nothing found during the previous steps.

CiscoDirSyncProcessFailedRetry

LDAPSync process failed on particular sync agreement.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

AgreementId [String] Reason [String]

Recommended Action

The sync process will automatic retry. See application logs for details.

CiscoDirSyncProcessFailedNoRetry

LDAPSync process failed on particular sync agreement

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

AgreementId [String] Reason [String]

Recommended Action

See application logs for details, the application will try to sync again in the next scheduled time

CiscoDirSyncProcessConnectionFailed

LDAPSync process failed to connect to LDAP server.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

AgreementId [String] LDAPHost [String] Reason [String]

Recommended Action

Ensure that the LDAP server is online. If SSL is used, please make sure the required certificate is available on local CM server. The application will automatically retry

CiscoDirSyncDBAccessFailure

LDAPSync process failed to access local database.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

AgreementId [String] Reason [String]

Recommended Action

Ensure that the local CallManager database is working properly. The failed sync process will restart at the next scheduled time.

CiscoLicenseManagerDown

License Manager Down and license provisioning will fail.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Reason [String]

Recommended Action

Restart License Manager service on specified node

CiscoLicenseRequestFailed

License Request Unsuccessful because it cannot fulfill the request.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Reason [String]

Recommended Action

See application logs for error

CiscoLicenseDataStoreError

License Database error because it cannot fulfill the request.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Reason [String]

Recommended Action

See application logs for error.

CiscoLicenseInternalError

Licensing Internal Error.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Reason [String]

Recommended Action

See application logs for error.

CiscoLicenseFileError

License File Error due to an invalid or tampered license file.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Reason [String]

Recommended Action

See application logs, verify that the license file is proper.

CLM_MsgIntChkError

ClusterMgr message integrity check error. ClusterMgr has received a message which has failed a message integrity check. This can be an indication that another node in the cluster is configured with the wrong security password.

Facility/Sub-Facility

CCM_CLUSTERMANAGER/CLUSTERMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Cluster Manager

Severity

Error (3)

Operating System

Appliance

Parameters

Sender IP address(String)

Recommended Action

Verify message is coming from an expected IP address. Verify the security password on that node.

CLM_UnrecognizedHost

ClusterMgr unrecognized host. ClusterMgr has received a message from an IP address which is not configured as a node in this cluster.

Facility/Sub-Facility

CCM_CLUSTERMANAGER/CLUSTERMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Cluster Manager

Severity

Error (3)

Operating System

Appliance

Parameters

Node IP address(String)

Recommended Action

Verify that this IP address is currently configured as a server in this cluster.

ConfigItAllBuildFilesFailed

A complete rebuild of all device configuration files has failed. Probable causes of this alarm could be failure to access the Cisco Unified Communications Manager database, or misconfiguration of some devices.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kConfigItAllBuildFilesFailed.
8.0(1)	Severity changed from Informational to Error.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Error

Recommended Action

In Cisco Unified Serviceability, enabled Detailed level traces in the Trace Configuration window for TFTP and Cisco Database Layer Monitor services. Also, use RTMT to look for errors that may have occurred around the time of the alarm.

ConfigItAllReadConfigurationFailed

Failed to retrieve enterprise parameter values from database when rebuilding all configuration files. This is usually caused by a failure to access the Cisco Unified Communications Manager database.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kConfigItAllReadConfigurationFailed.
8.0(1)	Severity changed from Informational to Error.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Error

Recommended Action

In Cisco Unified Serviceability, enable Detailed level traces in the Trace Configuration window for TFTP and Cisco Database Layer Monitor services. Also, use RTMT to look for errors that may have occurred around the time of the alarm.

ConfigThreadBuildFileFailed

Failed to build all device configuration files at TFTP service startup. This is usually caused by database access failure.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kConfigThreadBuildFileFailed
8.0(1)	Severity changed from Informational to Error.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Error

Recommended Action

In Cisco Unified Serviceability, enable Detailed level traces in the Trace Configuration window for TFTP and Cisco Database Layer Monitor services. Also, use RTMT to look for errors that may have occurred around the time of the alarm.

ConfigThreadCNCMGrpBuildFileFailed

Failed to rebuild configuration files for changes in Cisco Unified Communications Manager Group settings. This is usually caused by a failure to access the Cisco Unified Communications Manager database.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kConfigThreadCNCMGrpBuildFileFailed.
8.0(1)	Severity changed from Informational to Error.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Error

Recommended Action

In Cisco Unified Serviceability, enable Detailed level traces in the Trace Configuration window for TFTP and Cisco Database Layer Monitor services. Also, use RTMT to look for errors that may have occurred around the time of the alarm.

ConfigThreadCNGrpBuildFileFailed

Failed to rebuild configuration files for changes at group level settings such as Device Pool or Common Device Config settings. This is usually caused by a failure to access the Cisco Unified Communications Manager database.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kConfigThreadCNGrpBuildFileFailed.
8.0(1)	Severity changed from Informational to Error.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Error

Recommended Action

In Cisco Unified Serviceability, enable Detailed level traces in the Trace Configuration window for TFTP and Cisco Database Layer Monitor services. Also, use RTMT to look for errors that may have occurred around the time of the alarm.

ConfigThreadReadConfigurationFailed

Failed to retrieve enterprise parameter values from database at TFTP service startup. This is usually caused by database access failure.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kConfigThreadReadConfigurationFailed.
8.0(1)	Severity changed from Informational to Error.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Error

Recommended Action

In Cisco Unified Serviceability, enable Detailed level traces in the Trace Configuration window for TFTP and Cisco Database Layer Monitor services. Also, use RTMT to look for errors that may have occurred around the time of the alarm.

ConfigThreadUnknownExceptionCaught

An exception is caught in the main processing routine. This alarm is sent in conjunction with other alarms for failure when building configuration files or when the TFTP service is attempting to retrieve the values in the system's enterprise parameters.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kConfigThreadUnknownExceptionCaught.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Error (3)

Recommended Action

In Cisco Unified Serviceability, enable Detailed level traces in the Trace Configuration window for TFTP service. Also, use RTMT to look for errors that may have occurred around the time of the alarm.

ConflictingDataIE

A call has been rejected because the incoming PRI/BRI Setup message had an invalid IE.

A call has been rejected because an incoming PRI/BRI Setup message contained an invalid Coding Standard value in the Bearer Capability information element (IE). Unified CM only accepts PRI/BRI Setup messages with Coding Standard values of 0 or 1. When an invalid IE is received, Unified CM rejects the call setup and issues this alarm.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Device Name(String)

Recommended Action

Notify the service provider responsible for sending the Setup message that an IE with Coding Standard values of 0 or 1 must be included in Setup messages.

ConnectionFailure

Cisco CallManager failed to open TLS connection for the indicated device. Possible reasons could be wrong “Device Security Mode” configured, wrong “X.509 Subject Name” configured or unsupported cipher algorithm.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error (3)

Parameters

Device Name. [String] IP Address [String] Device type. [Optional] [Enum]Device description [Optional]. [String] Reason code [Enum]

Recommended Action

Check the Security profile of the indicated device. Make sure “Device Security Mode” is either “Authenticated” or “Encrypted”. Make sure “X.509 Subject Name” field has the right content. It should match the Subject Name in the certificate from the peer. Unified CM only supports AES_128_SHA cipher algorithm. Let the peer regenerate its certificate with the right algorithm.

Related Topics

DeviceType Enum Definitions for ConnectionFailure, on page 124
Reason Code Enum Definitions for ConnectionFailure, on page 126

DeviceType Enum Definitions for ConnectionFailure

Value	Definition
1	CISCO_30SP+
2	CISCO_12SP+
3	CISCO_12SP
4	CISCO_12S
5	CISCO_30VIP
6	CISCO_7910
7	CISCO_7960
8	CISCO_7940
9	CISCO_7935
12	CISCO_ATA_186
20	SCCP_PHONE
61	H323_PHONE
72	CTI_PORT
115	CISCO_7941
119	CISCO_7971
131	SIP_TRUNK
255	UNKNOWN
302	CISCO_7989
307	CISCO_7911
308	CISCO_7941G_GE
309	CISCO_7961G_GE

Value	Definition
335	MOTOROLA_CN622
336	BASIC_3RD_PARTY_SIP_DEVICE
348	CISCO_7931
358	CISCO_UNIFIED_COMMUNICATOR
365	CISCO_7921
369	CISCO_7906
374	ADVANCED_3RD_PARTY_SIP_DEVICE
375	CISCO_TELEPRESENCE
404	CISCO_7962
412	CISCO_3951
431	CISCO_7937
434	CISCO_7942
435	CISCO_7945
436	CISCO_7965
437	CISCO_7975
446	CISCO_3911
468	CISCO_UNIFIED_MOBILE_COMMUNICATOR
478	CISCO_TELEPRESENCE_1000
479	CISCO_TELEPRESENCE_3000
480	CISCO_TELEPRESENCE_3200
481	CISCO_TELEPRESENCE_500
484	CISCO_7925
493	CISCO_9971
495	CISCO_6921

Value	Definition
496	CISCO_6941
497	CISCO_6961
20000	CISCO_7905
30002	CISCO_7920
30006	CISCO_7970
30007	CISCO_7912
30008	CISCO_7902
30016	CISCO_IP_COMMUNICATOR
30018	CISCO_7961
30019	CISCO_7936
30035	IP_STE

Reason Code Enum Definitions for ConnectionFailure

Code	Reason
1	AuthenticationError
2	InvalidX509NameInCertificate
4	InvalidTLSCipher

ConnectionFailureToPDP

A connection request from Unified CM to the policy decision point (PDP) failed. The failure may have been a result of the following conditions:

- Network error causing limited or no connectivity between Unified CM and the PDP
- Authentication errors when Unified CM established an HTTPS connection to the PDP
- PDP was not in service.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error(3)

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameters

Policy Decision Point(String)

The cause of the connection failure(String)

Recommended Action

Verify the network connectivity between Unified CM and the PDP by pinging the policy server host from Cisco Unified OS Administration and take steps to establish connectivity if it has been lost. If the connection failure is due to an authentication problem, verify that the valid certificate of the PDP has been imported to Cisco Unified OS Administration and certificates from every node in the Unified CM cluster have been imported to every node in the PDP. Also, check whether the PDP service is active.

CNFFBuffWriteToFilefopenfailed

Failed to create Config File on disk or update existing Config File on disk. This may happen if disk is full or the file is in use.

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kCNFFBuffWriteToFilefopenfailed.
8.0(1)	Severity changed from Informational to Error.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Error

Parameters

FileName [String]

Recommended Action

Using RTMT, check the disk utilization and correct any issue discovered. If you do not discover a disk space issue, try restarting the TFTP service from Cisco Unified Serviceability (Tools > Control Center - Feature Services). Stopping and restarting the TFTP service is useful because the Config File that the TFTP service is trying to save might be an existing file that is in use. If you still get this error, go to Cisco Unified Serviceability and enable Detailed level traces in the Trace Configuration window for the TFTP service and contact the Cisco Technical Assistance Center (TAC).

CNFFBuffWriteToFilefwritefailed

Failed to save Config File to disk. This may happen if disk is full or the file is in use.

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kCNFFBuffWriteToFilefwritefailed.
8.0(1)	Severity changed from Informational to Error.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Error

Parameters

FileName [String]

Recommended Action

Using RTMT, check the disk utilization and correct any issue discovered. If you do not discover a disk space issue, try restarting the TFTP service from Cisco Unified Serviceability (Tools > Control Center - Feature Services). Stopping and restarting the TFTP service is useful because the Config File that the TFTP service is trying to save might be an existing file that is in use. If you still get this error, go to Cisco Unified Serviceability and enable Detailed level traces in the Trace Configuration window for the TFTP service and contact the Cisco Technical Assistance Center (TAC).

CtiProviderOpenFailure

CTI application is unable to open the provider. The IP address is shown in either IPv4 or IPv6 format depending on the IP addressing mode of the application.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiProviderOpenFailure.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameter(s)

Login User Id(String)

Reason code.(Enum)

IPAddress(String)

IPV6Address(String)

Recommended Action

Review the reason code and the recommended action within the reason code.

Related Topics

Reason Code Enum Definitions for CtiProviderOpenFailure, on page 130

Reason Code Enum Definitions for CtiProviderOpenFailure

Value	Definition
0	Unknown
0x8CCC0075 (2362179701)	Login request to authenticate user has timed out. Possible causes include LDAP server misconfiguration such as LDAP server referrals misconfiguration or Unified CM node experiencing high CPU usage. Recommended action is to verify the CPU utilization is in the safe range for Unified CM (this can be monitored using RTMT via CPU Pegging Alert)
0x8CCC0060 (2362179680)	Directory login failed. Verify that credentials are not misconfigured, check the userID and password configured in the application matches with what is configured in Unified CM Admin under (**User Management** > **End User/Application User**)
0x8CCC005E (2362179678)	Directory is unavailable. Verify that the LDAP server is reachable from Unified CM node, make sure that the network connectivity between Unified CM and the LDAP server by pinging the LDAP server host from Cisco Unified OS Administration and take steps to establish connectivity if it has been lost
0x8CCC00D1 (2362179793)	Application is connecting to a non secure port but has security privileges enabled for the user associated with the application. Check the user group configuration for the user in Unified CM Admin under (**User Management** > **End User/Application User**), select the user and verify the associated permissions information
0x8CCC005F (2362179679)	Standard CTI Use permission is not enabled. Users associated with applications are required to be included in "Standard CTI Enabled" user group. Verify the user group configuration for the user in Unified CM Admin under (**User Management** > **End User/Application User**), select the user and review the associated permissions information
0x8CCC00D0 (2362179792)	User is not enabled for a secure connection but the application connecting to secure port. Consider the application configuration and security configuration for the user, for TAPI applications review the **Control Panel** > **Phone** and **Modem Options** > **Advanced** > **select a CiscoTSP** > **Configure...** > **Security** and disable "Secure Connection to CTIManager". For JTAPI applications from JTPrefs choose Security and disable **Enable Secure Connection**. Also check the user group configuration for the user in Unified CM Admin under (**User Management** > **End User/Application User**), select the user and verify the associated permissions information

DBLGetVersionInfoError

DBL GetVersionInfo function returned NULL.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Error (3)

Recommended Action

None

DeviceTypeMismatch

Device type mismatch between the information contained in the device TFTP config file and what is configured in the database for that device.

The device type indicated in the device configuration file does not match the database configuration. This could indicate that a change was made in the database configuration that failed to get updated at the device itself.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Following information is updated: • Enum Definitions for DBDeviceType • Enum Definitions for DeviceType

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error

Parameters

Database device type [Enum]Device type. [Enum]Name of device. [String]

Recommended Action

Check the Unified CM Database Status report in Cisco Unified Reporting to verify that database replication is working. You can also go to Real-Time Reporting Tool (RTMT) and check the Replication Status in the

Database Summary page. If status shows 2, then replication is working. Restart the phone to download a new configuration file from TFTP. Also, refer to the reason code definitions for additional recommended actions.

Related Topics

DBDeviceType Enum Definitions for DeviceTypeMismatch, on page 132
DeviceType Enum Definitions for DeviceTypeMismatch, on page 134

DBDeviceType Enum Definitions for DeviceTypeMismatch

Code	Device Type
1	CISCO_30SP+
2	CISCO_12SP+
3	CISCO_12SP
4	CISCO_12S
5	CISCO_30VIP
6	CISCO_7910
7	CISCO_7960
8	CISCO_7940
9	CISCO_7935
12	CISCO_ATA_186
20	SCCP_PHONE
61	H323_PHONE
72	CTI_PORT
115	CISCO_7941
119	CISCO_7971
255	UNKNOWN
302	CISCO_7989
307	CISCO_7911
308	CISCO_7941G_GE
309	CISCO_7961G_GE

Code	Device Type
335	MOTOROLA_CN622
336	BASIC_3RD_PARTY_SIP_DEVICE
348	CISCO_7931
358	CISCO_UNIFIED_COMMUNICATOR
365	CISCO_7921
369	CISCO_7906
374	ADVANCED_3RD_PARTY_SIP_DEVICE
375	CISCO_TELEPRESENCE
404	CISCO_7962
412	CISCO_3951
431	CISCO_7937
434	CISCO_7942
435	CISCO_7945
436	CISCO_7965
437	CISCO_7975
446	CISCO_3911
468	CISCO_UNIFIED_MOBILE_COMMUNICATOR
478	CISCO_TELEPRESENCE_1000
479	CISCO_TELEPRESENCE_3000
480	CISCO_TELEPRESENCE_3200
481	CISCO_TELEPRESENCE_500
484	CISCO_7925
493	CISCO_9971
495	CISCO_6921

Code	Device Type
496	CISCO_6941
497	CISCO_6961
20000	CISCO_7905
30002	CISCO_7920
30006	CISCO_7970
30007	CISCO_7912
30008	CISCO_7902
30016	CISCO_IP_COMMUNICATOR
30018	CISCO_7961
30019	CISCO_7936
30035	IP_STE

DeviceType Enum Definitions for DeviceTypeMismatch

Code	Device Type
1	CISCO_30SP+
2	CISCO_12SP+
3	CISCO_12SP
4	CISCO_12S
5	CISCO_30VIP
6	CISCO_7910
7	CISCO_7960
8	CISCO_7940
9	CISCO_7935
12	CISCO_ATA_186

Code	Device Type
20	SCCP_PHONE
61	H323_PHONE
72	CTI_PORT
115	CISCO_7941
119	CISCO_7971
255	UNKNOWN
302	CISCO_7989
307	CISCO_7911
308	CISCO_7941G_GE
309	CISCO_7961G_GE
335	MOTOROLA_CN622
336	BASIC_3RD_PARTY_SIP_DEVICE
348	CISCO_7931
358	CISCO_UNIFIED_COMMUNICATOR
365	CISCO_7921
369	CISCO_7906
374	ADVANCED_3RD_PARTY_SIP_DEVICE
375	CISCO_TELEPRESENCE
404	CISCO_7962
412	CISCO_3951
431	CISCO_7937
434	CISCO_7942
435	CISCO_7945
436	CISCO_7965

Code	Device Type
437	CISCO_7975
446	CISCO_3911
468	CISCO_UNIFIED_MOBILE_COMMUNICATOR
478	CISCO_TELEPRESENCE_1000
479	CISCO_TELEPRESENCE_3000
480	CISCO_TELEPRESENCE_3200
481	CISCO_TELEPRESENCE_500
484	CISCO_7925
493	CISCO_9971
495	CISCO_6921
496	CISCO_6941
497	CISCO_6961
20000	CISCO_7905
30002	CISCO_7920
30006	CISCO_7970
30007	CISCO_7912
30008	CISCO_7902
30016	CISCO_IP_COMMUNICATOR
30018	CISCO_7961
30019	CISCO_7936
30035	IP_STE

DbInfoCorrupt

Database information returned is corrupt. Database configuration error was encountered.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Name of Device(String)

Recommended Action

Investigate configuration for the identified device.

DbInfoError

Error in the database information retrieved. Database configuration error was encountered.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Name of Device(String)

Recommended Action

Investigate configuration for identified device.

DbInfoTimeout

Database Information request timed out. Timeout was encountered while trying to read database configuration.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Routing List

SDL

SDI

Event Log

Sys Log

Parameter(s)

Name of Device(String)

Recommended Action

Investigate configuration for identified device.

DeviceCloseMaxEventsExceeded

The TCP socket for the SCCP device has been closed due to excessive events in a 5-second period. Under normal conditions, the device will reregister automatically.

The indicated SCCP device exceeded the maximum number of events allowed per-SCCP device. Events can be phone calls, KeepAlive messages, or excessive SCCP or non-SCCP messages. The maximum number of allowed events is controlled by the Cisco CallManager service parameter, Max Events Allowed. When an individual device exceeds the number configured in that service parameter, Unified CM closes the TCP connection to the device; automatic reregistration generally follows. This action is an attempt to stop malicious attacks on Unified CM or to ward off excessive CPU usage.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error (3)

Parameters

Total Events Received [UInt] IP Address [String] TCP Handle [String] Max Events Allowed [UInt] Number Of Skinny Device Throttled [UInt]

Recommended Action

Check the CCM trace data for the indicated SCCP device to determine the reason for the high number of events. Confirm that the value configured in the Cisco CallManager service parameter, Max Events Allowed, is a suitable number for your deployment.

DeviceInitTimeout

Device initialization timeout occurred. This alarm does not occur under normal working conditions; it will only occur if a device fails to respond to an initialize request.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error (3)

Parameters

Device Name [String] Protocol [String] Side Number [UInt]

Recommended Action

Investigate the identified device.

DirSyncSchedulerFailedToUpdateNextExecTime

Scheduler failed to update next execution time.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Message [String]

Recommended Action

Check the DirSync configuration and logs

DirSyncScheduledTaskFailed

Directory synchronization task failed.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

SchedulerID [String] ErrorMessage [String]

Recommended Action

Check the DirSync configuration and logs

DirSyncSchedulerFailedToGetDBSchedules

Failed to get directory synchronization schedules from DB.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Message [String]

Recommended Action

Check the DirSync configuration and logs.

DirSyncSchedulerInvalidEventReceived

Invalid event received by DirSync scheduler from database.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Action [String] Message [String]

Recommended Action

Check the DirSync configuration and logs

DirSyncInvalidScheduleFound

Invalid schedule read by DirSync scheduler from database.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

ScheduleID [String]

Recommended Action

Check the DirSync configuration and logs

DirSyncSchedulerFailedToRegisterDBEvents

DirSync scheduler failed to register DB notifications.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

ScheduleTable [String]

Recommended Action

Check the DirSync configuration and logs

DirSyncSchedulerEngineFailedToStart

DirSync scheduler engine failed to start.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

ScheduleTable [String]

Recommended Action

Check the DirSync configuration and logs

DirSyncScheduleDeletionFailed

DirSync schedule deletion request failed.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

ScheduleID [String]

Recommended Action

Check the DirSync configuration and logs

DirSyncScheduleUpdateFailed

DirSync schedule update request failed.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

ScheduleID [String]

Recommended Action

Check the DirSync configuration and logs.

DRFMasterAgentStartFailure

DRF Master Agent was unable to start because it was unable to open port 4040.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	New name changed from CiscoDRFMasterAgentStartFailure. Routing List elements added. Descriptive text and recommended action changed.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error

Routing List

Event Log

Sys Log

Parameters

Reason [String]

Recommended Action

Check if port 4040 is not already in use.

DRFLocalAgentStartFailure

DRF Local Agent was not able to start because it was unable to connect to the Master Agent on port 4040.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	New name changed from CiscoDRFLocalAgentStartFailure. Routing List elements added. Descriptive text and recommended action changed.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason [String]

Recommended Action

Check if the CiscoDRFMaster and CiscoDRFLocal services are running.

DRFRestoreFailure

DRF Restore process encountered errors.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	New name changed from CiscoDRFRestoreFailure. Routing List elements added. Descriptive text and recommended action changed.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event log

Sys Log

Parameters

Reason [String]

Recommended Action

Check DRF logs for further details.

DRFInternalProcessFailure

DRF internal process has some problems.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	New name changed from CiscoDRFInternalProcessFailure. Routing list added and recommended action changed.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason [String]

Recommended Action

Check DRF logs for details.

DRFTruststoreMissing

DRF uses ipsec truststore certificate for securing communication between the MA and LA service. This certificate is missing on the node, DRF LA will not be able to connect to MA.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFTruststoreMissing. Routing List elements added.
7.0(1)	Error message removed.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Download ipsec.pem file from Publisher and upload it as ipsec-trust only on the missing node then restart Cisco DRF Local service.

DRFUnknownClient

The DRF Master Agent running on the Publisher has received a Client connection request from an unknown server outside the cluster.The request has been rejected.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFUnknownClient. Routing List elements added.
7.0(1)	Error message removed.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Remove the suspect server from the network. Refer to the Reason section for suspect servers: Hostname and IP Address.

DRFSecurityViolation

The DRF System has detected a malicious pattern which could result in a security violation. The DRF Network Message contains a malicious pattern which could result in a security violation like code injection or directory traversal. DRF Network Message has been blocked.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFSecurityViolation. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Stop the Cisco DRF Master and Cisco DRF Local Agent Services.

DRFBackupDeviceError

DRF Backup process is failed due to backup device error.

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFBackupDeviceError. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Check if the proper device has been specified in the DRF configurations.

DRFTapeDeviceError

DRF is unable to access tape device.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFTapeDeviceError. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Check if tape drive is working properly and it contains a valid tape.

DRFRestoreInternalError

DRF Restore operation has encountered an error. Restore cancelled internally.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFRestoreInternalError. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Check DRF logs for details.

DRFMABackupComponentFailure

DRF was unable to backup at least one component because of an error.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFMABackupComponentFailure. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Check the component backup logs and contact support if needed.

DRFMARestoreComponentFailure

DRF was unable to restore at least one component due to an error.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFMARestoreComponentFailure. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Check the component restore logs and contact support if needed.

DRFMABackupNodeDisconnect

The DRF Master Agent was running a backup operation on a CCM cluster, when one of the nodes disconnected before the backup operation was completed.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFMABackupNodeDisconnect. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Check the computer that disconnected during backup. If the computer was accidentally shutdown, restart the backup.

DRFNoRegisteredComponent

No registered components available, backup failed.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFNoRegisteredComponent. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Ensure at least one component is registered before attempting a backup.

DRFNoRegisteredFeature

No feature selected for backup.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFNoRegisteredComponent. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Ensure at least one feature is configured before attempting a backup.

DRFMARestoreNodeDisconnect

The node being restored disconnected from the Master Agent prior to being fully restored.

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFMARestoreNodeDisconnect. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Check the computer that disconnected during restore. If the computer was accidentally shutdown, restart the restore.

DRFSftpFailure

DRF (s)FTP operation has failed.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFSftpFailure. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Ensure that the destination server is available, has appropriate permissions and (s)FTP daemon is running.

DRFRegistrationFailure

DRF Registration operation failed due to an internal error.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFRegistrationFailure. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Check the DRF logs and contact support if needed.

DRFBackupCancelInternalError

DRF Backup operation has encountered an error. Backup cancelled internally.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFBackupCancelInternalError. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Check DRF logs for details.

DRFLogDirAccessFailure

DRF could not access the log directory.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFLogDirAccessFailure. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Ensure that the DRF user has required permission/enough space on DRF Log and Trace directory.

DRFFailure

DRF Backup or Restore process has failed because it encountered errors.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFFailure. Changed Routing List element Data Collector to Alert Manager and added Sys Log.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Error (3)

Routing List

Event Log

Alert Manager

Sys Log

Parameters

Reason(String)

Recommended Action

Check DRF logs for further details.

DRFLocalDeviceError

DRF unable to access local device.

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

ERROR

Routing List

Event Log

Sys Log

Parameter(s)

Reason(String)

Recommended Action

Check if local location exists and is accessible.

DuplicateLearnedPattern

This alarm occurs when CCD requesting service received a duplicate Hosted DN.

The Call Control Discovery (CCD) requesting service received the same hosted DN from multiple call control entities such as Unified CM Express or another Unified CM cluster. The Cisco CallManager service parameter, Issue Alarm for Duplicate Learned Patterns, controls whether this alarm gets issued.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Client Handle(String)

Service ID(UInt)

Sub Service ID(UInt)

InstanceID1(UInt)

InstancID2(UInt)

InstanceID3(UInt)

InstanceID4(UInt)

Recommended Action

In RTMT, check the Pattern Report (**CallManager** > **Report** > **Learned Pattern**) and look for the duplicate pattern identified in this alarm. Learned patterns must be unique. Determine which call control entity (such as Unified CM or Unified CM Express) needs to be changed so that there is no duplicate pattern. Refer to the call control entity's configuration guide (help text) to learn how to update a hosted DN pattern. In Unified CM, to change the Hosted DN Pattern go to Cisco Unified CM Administration to update the Hosted DN Pattern configuration (**Call Routing** > **Call Control Discovery** > **Hosted DN Patterns**).

EMAppInitializationFailed

EM Application not started. Error occurred while starting application.

Cisco Unified Serviceability Alarm Definition Catalog

System/EMAlarmCatalog

Severity

ERROR

Routing List

Sys Log

Event Log

Data Collector

Parameter(s)

Servlet Name(String)

Recommended Action

Action See application logs for error. Default location for the logs are at /var/log/active/tomcat/logs/em/log4j/

EMCCFailedInLocalCluster

EMCC login failure occurred due to one of the following conditions:

- Devices are incompatible with EMCC.
- Unable to retrieve remote cluster information.

- EMCC is restricted by the local cluster.
- Untrusted certificate received from the remote end while trying to establish a connection

Reason Codes:

- 31—User is not enabled for EMCC
- 211/38—EMCC or PSTN is not activated in InterClusterServiceProfile page
- 23—User does not exist in the end user table
- 35—No remote cluster entry is present for the home cluster

Cisco Unified Serviceability Alarm Definition Catalog

System/EMAlarmCatalog

Severity

ERROR(3)

Routing List

Sys Log

Event Log

Alert Manager

Parameters

Device Name(String)

Login Date/Time(String)

Login UserID(String)

Reason(String)

Recommended Action

Perform the following:

1. Validate if the device model supports EMCC.
2. Ensure that every remote cluster added for EMCC has valid hostname/IP address for EM and PSTN access in the Remote Cluster administration window (From Unified CM Administration window, go to **System** > **EMCC** > **Remote Cluster**).
3. Ensure that the entries are enabled.
4. Ensure that a bundle of all Tomcat certificates (PKCS12) has been imported into the local tomcat-trust keystore (From the OS Administration window, go to **Security** > **Certificate Management** and check the certificates in tomcat-trust).

EMServiceConnectionError

EM Service not reachable. EM Service might be down in one or more nodes in the cluster.

Cisco Unified Serviceability Alarm Definition Catalog

System/EMAlarmCatalog

Severity

ERROR

Routing List

Sys Log

Event Log

Parameter(s)

Servlet Name(String)

Recommended Action

Check if Cisco Extension Mobility service is running on all nodes of the cluster where the service is activated.

EndPointTransientConnection

End point transient connection attempt.

A connection was established and immediately dropped before completing registration. Incomplete registration may indicate that a device is rehoming in the middle of registration. The alarm could also indicate a device misconfiguration, database error, or an illegal/unknown device trying to attempt a connection. Network connectivity problems can affect device registration, or the restoration of a primary Unified CM may interrupt registration.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Data Collector

SNMP Traps

Alternate Syslog

Parameter(s)

Device IP address(String)

Device name(String)

Device MAC address(String)

Protocol(String)

Device type(Enum)

Reason Code(Enum)

Connecting Port(UInt)

Registering SIP User(String)

IPv6Address(String)

IPAddressAttributes(Enum)

IPv6AddressAttributes(Enum)

Recommended Action

Investigate any network connectivity problems in the system. It's possible that you have reached the maximum number of devices; the Cisco Unified Communications Manager service parameter, Maximum Number of Registered Devices, controls the number of devices allowed in the system. Taking licensing, system hardware and other related concerns into consideration, you could increase the value of the service parameter. Also, refer to the reason code definitions for recommended actions. No action is required if this event was issued as a result of a normal device rehome.

Related Topics

Device Type Enum Definitions for EndPointTransientConnection, on page 164
Reason Code Enum Definitions for EndPointTransientConnection, on page 167
IPAddressAttributes Enum Definitions for EndPointTransientConnection, on page 170
IPv6AddressAttributes Enum Definitions for EndPointTransientConnection, on page 171

Device Type Enum Definitions for EndPointTransientConnection

Value	Definition
1	CISCO_30SP+
2	CISCO_12SP+
3	CISCO_12SP
4	CISCO_12S
5	CISCO_30VIP
6	CISCO_7910

Value	Definition
7	CISCO_7960
8	CISCO_7940
9	CISCO_7935
12	CISCO_ATA_186
20	SCCP_PHONE
61	H323_PHONE
72	CTI_PORT
115	CISCO_7941
119	CISCO_7971
255	UNKNOWN
302	CISCO_7989
307	CISCO_7911
308	CISCO_7941G_GE
309	CISCO_7961G_GE
335	MOTOROLA_CN622
336	BASIC_3RD_PARTY_SIP_DEVICE
348	CISCO_7931
358	CISCO_UNIFIED_COMMUNICATOR
365	CISCO_7921
369	CISCO_7906
374	ADVANCED_3RD_PARTY_SIP_DEVICE
375	CISCO_TELEPRESENCE
404	CISCO_7962
412	CISCO_3951

Value	Definition
431	CISCO_7937
434	CISCO_7942
435	CISCO_7945
436	CISCO_7965
437	CISCO_7975
446	CISCO_3911
468	CISCO_UNIFIED_MOBILE_COMMUNICATOR
478	CISCO_TELEPRESENCE_1000
479	CISCO_TELEPRESENCE_3000
480	CISCO_TELEPRESENCE_3200
481	CISCO_TELEPRESENCE_500
484	CISCO_7925
493	CISCO_9971
495	CISCO_6921
496	CISCO_6941
497	CISCO_6961
20000	CISCO_7905
30002	CISCO_7920
30006	CISCO_7970
30007	CISCO_7912
30008	CISCO_7902
30016	CISCO_IP_COMMUNICATOR
30018	CISCO_7961
30019	CISCO_7936

Value	Definition
30035	IP_STE

Reason Code Enum Definitions for EndPointTransientConnection

Value	Definition
1	Unknown—(SCCP only) The device failed to register for an unknown reason. If this persists, collect SDL/SDI traces with “Enable SCCP Keep Alive Trace” enabled and contact TAC.
2	NoEntryInDatabase—(MGCP only) The device is not configured in the Cisco Unified CM database and auto-registration is either not supported for the device type or is not enabled. To correct this problem, configure this device via Cisco Unified CM Administration.
3	DatabaseConfigurationError—The device is not configured in the Cisco Unified CM database and auto-registration is either not supported for the device type or is not enabled. To correct this problem, configure this device via Cisco Unified CM Administration.
4	DeviceNameUnresolveable—For SIP third-party devices, this reason code means that Cisco Unified CM could not determine the name of the device from the Authorization header in the REGISTER message. The device did not provide an Authorization header after Cisco Unified CM challenged with a 401 Unauthorized message. Verify the device is configured with digest credentials and is able to respond to 401 challenges with an Authorization header. If this is a Cisco IP phone, the configuration may be out-of-sync. First go to the Cisco Unified Reporting web page, generate a Unified CM Database Status report, and verify “all servers have a good replication status”. If DB replications looks good, reset the phone. If that still doesn't fix the problem, restart the TFTP and the Cisco CallManager services. For all other devices, this reason code means that DNS lookup failed. Verify the DNS server configured via the OS Administration CLI is correct and that the DNS name used by the device is configured in the DNS server.
5	maxDevRegExceeded—Maximum number of device registrations have been reached.
6	ConnectivityError - The network connection between the device and Cisco Unified CM dropped before the device was fully registered. Possible causes include device power outage, network power outage, network configuration error, network delay, packet drops and packet corruption. It is also possible to get this error if the Cisco Unified CM node is experiencing high CPU usage. Verify the device is powered up and operating, verify network connectivity between the device and Cisco Unified CM, and verify the CPU utilization is in the safe range (this can be monitored using RTMT via CPU Pegging Alert).

Value	Definition
7	InitializationError—An internal error occurred within Cisco Unified CM while processing the device registration. It is recommended to restart the Cisco CallManager service. If this occurs repeatedly, collect SDL/SDI detailed traces with “Enable SIP Keep Alive (REGISTER Refresh) Trace” and “Enable SCCP Keep Alive Trace” under Cisco CallManager services turned on and contact TAC.
8	DeviceInitiatedReset—Indicates that the error was due to device initiated reset.
9	CallManagerReset—Indicates that the error was due to call manager reset.
10	AuthenticationError—The device failed either TLS or SIP digest security authentication. If the device is a SIP phone and is enabled for digest authentication (on the **System** > **Security Profile** > **Phone Security Profile**, check if “Enable Digest Authentication” checkbox is checked), verify the “Digest Credentials” in the End User config page are configured. Also, check the phone config page to see if the phone is associated with the specified end user in the Digest User drop box. If the device is a third-party SIP device, verify the digest credentials configured on the phone match the “Digest Credentials” configured in the End User page.
11	InvalidX509NameInCertificate—Configured “X.509 Subject Name” doesn't match what is in the certificate from the device. Check the Security Profile of the indicated device and verify the “Device Security Mode” is either “Authenticated” or “Encrypted”. Verify the “X.509 Subject Name” field has the right content. It should match the Subject Name in the certificate from the peer.
12	InvalidTLSCipher—Unsupported cipher algorithm used by the device; Cisco Unified CM only supports AES_128_SHA cipher algorithm. Recommended action is for the device to regenerate its certificate with the AES_128_SHA cipher algorithm.
13	DirectoryNumberMismatch—Indicates mismatch between the directory number that the SIP device is trying to register with and the directory number configured in the Cisco Unified CM for the SIP device.
14	MalformedRegisterMsg—(SIP only) A SIP REGISTER message could not be processed because of an illegal format. Possible causes include a missing Call-ID header, a missing AoR in the To header, and an expires value too small. Verify the REGISTER message does not suffer from any of these ills.

Value	Definition
15	ProtocolMismatch—The protocol of the device (SIP or SCCP) does not match the configured protocol in Cisco Unified CM. Recommended actions: **1** Verify the device is configured with the desired protocol. **2** Verify the firmware load ID on the Device Defaults page is correct and actually exists on the TFTP server **3** If there is a firmware load ID configured on the device page, verify it is correct and exists on the TFTP server (On Cisco Unified OS Administration page, **Software Upgrades** > **TFTP File Management**, look for the file name as specified by load ID). **4** Restart the TFTP and Cisco CallManager services. Use the Cisco Unified OS Administration TFTP File Management page to verify the configured firmware loads exist.
16	DeviceNotActive—The device has not been activated.
17	AuthenticatedDeviceAlreadyExists—A device with the same name is already registered. If this occurs repeatedly, collect SDL/SDI detailed traces with "Enable SIP Keep Alive (REGISTER Refresh) Trace" and "Enable SCCP Keep Alive Trace" under Cisco CallManager services turned on and contact TAC. There may be an attempt by unauthorized devices to register.
18	ObsoleteProtocolVersion—(SCCP only) A SCCP device registered with an obsolete protocol version. Power cycle the phone. Verify that the TFTP service is activated. Verify that the TFTP server is reachable from the device. If there is a firmware load ID configured on the Phone Config page, verify that the firmware load ID exists on the TFTP server (On Cisco Unified OS Administration page, **Software Upgrades** > **TFTP File Management**, look for the file name as specified by load ID).
23	DatabaseTimeout—Cisco Unified CM requested device configuration data from the database but did not receive a response within 10 minutes.
25	RegistrationSequenceError—(SCCP only) A device requested configuration information from the Cisco Unified CM at an unexpected time. The Cisco Unified CM had not yet obtained the requested information.
26	InvalidCapabilities— (SCCP only) Cisco Unified CM detected an error in the media capabilities reported by the device during registration. The device reported the capabilities in the StationCapabilitiesRes message.
27	CapabilityResponseTimeout— (SCCP only) Cisco Unified CM timed out while waiting for the device to respond to a request to report its media capabilities.

Value	Definition
28	SecurityMismatch—Cisco Unified CM detected a mismatch in the security settings of the device and/or the Unified CM. The following mismatches are detected: **1** The device established a secure connection, yet reported that it does not have the ability to do authenticated signaling. **2** The device did not establish a secure connection, but the security mode configured for the device indicates that it should have done so. **3** The device established a secure connection, but the security mode configured for the device indicates that it should not have done so.
29	AutoRegisterDBError—(SCCP only) Auto-registration of a device failed for one of the following reasons: **1** Auto-registration is not allowed for the device type. **2** An error occurred in the auto-registration stored procedure.
30	DBAccessError—(SCCP only) Auto-registration of a device failed because of an error that occurred while building the station registration profile.
31	AutoRegisterDBConfigTimeout—(SCCP only) Cisco Unified CM timed out during auto-registration of a device. The registration profile of the device did not get inserted into the database in time.
32	DeviceTypeMismatch—(SCCP only) The device type reported by the device does not match the device type configured on the Cisco Unified CM.
33	AddressingModeMismatch—(SCCP only) Cisco Unified CM detected an error related to the addressing mode configured for the device. One of the following errors was detected: **1** The device is configured to use only IPv4 addressing, but did not specify an IPv4 address. **2** The device is configured to use only IPv6 addressing, but did not specify an IPv6 address.

IPAddressAttributes Enum Definitions for EndPointTransientConnection

Value	Definition
0	Unknown—The device has not indicated what this IPv4 address is used for
1	Administrative only—The device has indicated that this IPv4 address is used for administrative communication (web interface) only

Value	Definition
2	Signal only—The device has indicated that this IPv4 address is used for control signaling only
3	Administrative and signal—The device has indicated that this IPv4 address is used for administrative communication (web interface) and control signaling

IPv6AddressAttributes Enum Definitions for EndPointTransientConnection

Value	Definition
0	Unknown—The device has not indicated what this IPv6 address is used for
1	Administrative only—The device has indicated that this IPv6 address is used for administrative communication (web interface) only
2	Signal only—The device has indicated that this IPv6 address is used for control signaling only
3	Administrative and signal—The device has indicated that this IPv6 address is used for administrative communication (web interface) and control signaling

EndPointUnregistered

An endpoint that has previously registered with Cisco Unified Communications Manager has unregistered. In cases of normal unregistration with reason code “CallManagerReset”, “CallManagerRestart”, “DeviceInitiatedReset”, “EMLoginLogout”, or “EMCCLoginLogout”, the severity of this alarm is lowered to INFORMATIONAL. An endpoint can unregister for many reasons, both intentional, such as manually resetting the device after a configuration change, or unintentional, such as loss of network connectivity. Other causes for this alarm could include a phone being registered to a secondary node and then the primary node come back online, causing the phone to rehome to the primary Cisco Unified CM node or lack of a KeepAlive being returned from the Cisco Unified CM node to which this endpoint was registered. Unregistration also occurs if Cisco Unified CM receives a duplicate registration request for this same device.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Data Collector

SNMP Traps

Alternate Syslog

Parameter(s)

Device name(String)

Device MAC address(String)

Device IP address(String)

Protocol(String)

Device type(Enum)

Device description(String)

Reason Code(Enum)

IPV6Address(String)

IPAddressAttributes(Enum)

IPV6AddressAttributes(Enum)

Recommended Action

Actions to take vary depending on the reason specified for the endpoint unregistration. If the reason is ConfigurationMismatch, go to the Device Configuration page in Cisco Unified CM Administration, make a change to the Description field for this device, click Save, then reset the device. In the case of a network connectivity or loss of KeepAlives problem, use network diagnostic tools and the Cisco Unified CM Reporting tool to fix any reported network or Unified CM system errors. In the case of an endpoint rehoming to the primary Unified CM node, watch for a successful registration of the device on the primary node. In the case of a duplicate registration request, it may be a non-malicious occurrence due to timing of an endpoint registering and unregistering; if duplicate registration requests continue or if the same endpoint has different IP addresses, confirm the IP address on the physical device itself by checking the settings on the device (settings button). If unregistration of this device was expected, no action is required. Also, refer to the reason code descriptions for recommended actions.

Related Topics

Device Type Enum Definitions for EndPointUnregistered, on page 172
Reason Code Enum Definitions for EndPointUnregistered, on page 175
IPAddressAttributes Enum Definitions for EndPointUnregistered, on page 178
IPV6AddressAttributes Enum Definitions for EndPointUnregistered, on page 178

Device Type Enum Definitions for EndPointUnregistered

Value	Definition
1	CISCO_30SP+

Value	Definition
2	CISCO_12SP+
3	CISCO_12SP
4	CISCO_12S
5	CISCO_30VIP
6	CISCO_7910
7	CISCO_7960
8	CISCO_7940
9	CISCO_7935
12	CISCO_ATA_186
20	SCCP_PHONE
61	H323_PHONE
72	CTI_PORT
115	CISCO_7941
119	CISCO_7971
255	UNKNOWN
302	CISCO_7989
307	CISCO_7911
308	CISCO_7941G_GE
309	CISCO_7961G_GE
335	MOTOROLA_CN622
336	BASIC_3RD_PARTY_SIP_DEVICE
348	CISCO_7931
358	CISCO_UNIFIED_COMMUNICATOR
365	CISCO_7921

Value	Definition
369	CISCO_7906
374	ADVANCED_3RD_PARTY_SIP_DEVICE
375	CISCO_TELEPRESENCE
404	CISCO_7962
412	CISCO_3951
431	CISCO_7937
434	CISCO_7942
435	CISCO_7945
436	CISCO_7965
437	CISCO_7975
446	CISCO_3911
468	CISCO_UNIFIED_MOBILE_COMMUNICATOR
478	CISCO_TELEPRESENCE_1000
479	CISCO_TELEPRESENCE_3000
480	CISCO_TELEPRESENCE_3200
481	CISCO_TELEPRESENCE_500
484	CISCO_7925
493	CISCO_9971
495	CISCO_6921
496	CISCO_6941
497	CISCO_6961
20000	CISCO_7905
30002	CISCO_7920
30006	CISCO_7970

Value	Definition
30007	CISCO_7912
30008	CISCO_7902
30016	CISCO_IP_COMMUNICATOR
30018	CISCO_7961
30019	CISCO_7936
30035	IP_STE

Reason Code Enum Definitions for EndPointUnregistered

Value	Definition
1	Unknown—The device has unregistered for an unknown reason. If the device does not reregister within 5 minutes, verify it is powered-up and verify network connectivity between the device and Cisco Unified CM.
2	NoEntryInDatabase—Device not configured properly in the Cisco Unified CM database.
3	DatabaseConfigurationError—Device configuration error in the Cisco Unified CM database.
4	DeviceNameUnresolveable—The Cisco Unified CM is unable to resolve the device name to an IP Address internally.
5	MaxDevRegExceeded—Maximum number of device registrations have been reached.
6	ConnectivityError—Network communication between the device and Cisco Unified CM has been interrupted. Possible causes include device power outage, network power outage, network configuration error, network delay, packet drops and packet corruption. It is also possible to get this error if the Cisco Unified CM node is experiencing high CPU usage. Verify the device is powered up and operating, verify network connectivity between the device and Cisco Unified CM, and verify the CPU utilization is in the safe range (this can be monitored using RTMT via CPU Pegging Alert).
7	InitializationError—Indicates that an error occurred when the Cisco Unified CM tries to initialize the device.
8	DeviceInitiatedReset—The device has initiated a reset, possibly due to a power cycle or internal error. No action required; the device will reregister automatically.

Value	Definition
9	CallManagerReset—A device reset was initiated from Cisco Unified CM Administration, either due to an explicit command from an administrator, or due to internal errors encountered. No action necessary, the device will reregister automatically.
10	DeviceUnregistered—The device has explicitly unregistered. Possible causes include a change in the IP address or port of the device. No action is necessary, the device will reregister automatically.
11	MalformedRegisterMsg—(SIP only) A SIP REGISTER message could not be processed because of an illegal format. Possible causes include a missing Call-ID header, a missing AoR in the To header, and an expires value too small. Verify the REGISTER message does not suffer from any of these ills.
12	SCCPDeviceThrottling—(SCCP only) The indicated SCCP device exceeded the maximum number of events allowed per-SCCP device. Events can be phone calls, KeepAlive messages, or excessive SCCP or non-SCCP messages. The maximum number of allowed events is controlled by the Cisco CallManager service parameter, Max Events Allowed. When an individual device exceeds the number configured in that service parameter, Unified CM closes the TCP connection to the device; automatic reregistration generally follows. This action is an attempt to stop malicious attacks on Unified CM or to ward off excessive CPU usage. No action necessary, the device will reregister automatically.
13	KeepAliveTimeout—A KeepAlive message was not received. Possible causes include device power outage, network power outage, network configuration error, network delay, packet drops and packet corruption. It is also possible to get this error if the Unified CM node is experiencing high CPU usage. Verify the device is powered up and operating, verify network connectivity between the device and Unified CM, and verify the CPU utilization is in the safe range (this can be monitored using RTMT via CPU Pegging Alert). No action necessary, the device will reregister automatically.
14	ConfigurationMismatch—(SIP only) The configuration on the device does not match the configuration in Unified CM. This can be caused by database replication errors or other internal Unified CM communication errors. First go to the Cisco Unified Reporting web page, generate a Unified CM Database Status report, and verify "all servers have a good replication status". If this device continues to unregister with this reason code, go to the Cisco Unified CMAdmin Device web page for the device and click Save. This allows a change notify to be generated to the Unified CM and TFTP services and rebuild a new config file. If the problem still persists, restart the TFTP service and Unified CM service.
15	CallManagerRestart—A device restart was initiated from Cisco Unified CM, either due to an explicit command from an administrator, or due to a configuration change such as adding, deleting or changing a DN associated with the device. No action necessary, the device will reregister automatically.
16	DuplicateRegistration—Cisco Unified CM detected that the device attempted to register to two nodes at the same time. Cisco Unified CM initiated a restart to the phone to force it to rehome to a single node. No action necessary, the device will reregister automatically.

Value	Definition
17	CallManagerApplyConfig—An ApplyConfig command was invoked from Unified CM Administration resulting in an unregistration. No action necessary, the device will reregister automatically.
18	DeviceNoResponse—The device did not respond to a reset or restart notification, so it is being forcefully reset. If the device does not reregister within 5 minutes, confirm it is powered-up and confirm network connectivity between the device and Cisco Unified CM.
19	EMLoginLogout —The device has been unregistered due to an Extension Mobility login or logout.
20	EMCCLoginLogout—The device has been unregistered due to an Extension Mobility Cross Cluster login or logout.
21	PowerSavePlus—The device powered off as a result of the Power Save Plus feature that is enabled for this device. When the device powers off, it remains unregistered from Unified CM until the Phone On Time defined in the Product Specific Configuration for this device.
22	CallManagerForcedRestart—(SIP Only) The device did not respond to an Apply Config request and as a result, Unified CM sent a restart request to the device. The device may be offline due to a power outage or network problem. Confirm that the device is powered-up and that network connectivity exists between the device and Unified CM.
23	SourceIPAddrChanged—(SIP Only) The device has been unregistered because the IP address in the Contact header of the REGISTER message has changed. The device will be automatically reregistered. No action is necessary.
24	SourcePortChanged—(SIP Only) The device has been unregistered because the port number in the Contact header of the REGISTER message has changed. The device will be automatically re-registered. No action is necessary.
25	RegistrationSequenceError—(SCCP only) A device requested configuration information from the Unified CM at an unexpected time. The Unified CM no longer had the requested information in memory.
26	InvalidCapabilities—(SCCP only) Unified CM detected an error in the updated media capabilities reported by the device. The device reported the capabilities in one of the StationUpdateCapabilities message variants.
28	FallbackInitiated—The device has initiated a fallback and will automatically reregister to a higher-priority Unified CM. No action is necessary.
29	DeviceSwitch—A second instance of an endpoint with the same device name has registered and assumed control. No action is necessary.

IPAddressAttributes Enum Definitions for EndPointUnregistered

Value	Definition
0	Unknown—The device has not indicated what this IPv4 address is used for
1	Administrative only—The device has indicated that this IPv4 address is used for administrative communication (web interface) only
2	Signal only—The device has indicated that this IPv4 address is used for control signaling only
3	Administrative and signal—The device has indicated that this IPv4 address is used for administrative communication (web interface) and control signaling

IPV6AddressAttributes Enum Definitions for EndPointUnregistered

Value	Definition
0	Unknown—The device has not indicated what this IPv6 address is used for
1	Administrative only—The device has indicated that this IPv6 address is used for administrative communication (web interface) only
2	Signal only—The device has indicated that this IPv6 address is used for control signaling only
3	Administrative and signal— The device has indicated that this IPv6 address is used for administrative communication (web interface) and control signaling

ErrorChangeNotifyClientTimeout

A change notification client was responding slowly and has been removed. A change notification recipient has not responded to change notification in several minutes and was thus removed. This may delay call processing features, such as call forwarding and so on.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Added Routing List elements and deleted Data Collector element.

Facility/Sub-Facility

CCM_DB_LAYER-DB

Cisco Unified Serviceability Alarm Definition Catalog

System/DB

Severity

Error (3)

Routing List

SDI

Event Log

Sys Log

Recommended Action

Rebooting the box will clear this situation. Alternatively, dbnotify trace could be analyzed to find the client that was removed and that service could be restarted in Cisco Unified Serviceability.

ErrorParsingDirectiveFromPDP

Cisco Unified Communications Manager (Unified CM) failed to parse the call routing directive or the diversion destination in the call routing response from the policy decision point (PDP).

A routing response was received but Cisco Unified Communications Manager (Unified CM) failed to parse the mandatory elements in the response. This means that a call routing directive or the call diversion destination could not be parsed correctly, or that the call routing directive was not recognized. The error may due to a syntax error or because the call routing directive is missing or the call diversion destination is missing in the call routing response.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Policy Decision Point(String)

Called Party Number(String)

Calling Party Number(String)

Calling User Id(String)

Response XML Data(String)

Recommended Action

Check the external call control documentation, including any applicable API documentation, to determine whether the call routing directive that was included as part of the policy obligations in the call routing response are correctly entered according to the information defined in the external call control documentation.

ErrorReadingInstalledRPMS

Could not read installed RPMs to populate component version table. The function that reads the RPM version information and populates database failed.

Facility/Sub-Facility

CCM_DB_LAYER-DB

Cisco Unified Serviceability Alarm Definition Catalog

System/DB

Severity

Error (3)

Recommended Action

Report this error to the administrator.

FailureResponseFromPDP

The policy decision point (PDP) returned a 4xx (client) or 5xx (server) status code in the HTTP response.

Cisco Unified Communications Manager (Unified CM) received a 4xx or 5xx response from the policy decision point (PDP). A 4xx response indicates errors in the call routing request from Unified CM, for example: a 400 response indicates the call routing request could not be understood by the PDP; a 404 indicates that the PDP did not find a matching request URI. A 5xx error indicates a PDP server error, for example: a 500 response indicates a PDP internal error; A 501 response indicates that the PDP does not support the functionality to generate a call routing response; a 503 indicates that the PDP is busy and temporarily cannot generate a response; a 505 indicates that the HTTP version number included in the call routing request from Unified CM is not supported. Other such errors may be responsible; please refer to generally available guidelines on HTTP or check the RFC 2616 for detailed explanations about HTTP Status Code definitions.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Policy Decision Point(String)

The status code and reason phrase for the failure(String)

Recommended Action

If a 4xx response caused the alarm, verify that the PDP has been accurately configured for the functionality and call routing that you expect it to perform. If a 500 response causes the alarm, check whether the PDP service is active and check the PDP server's log files for any errors. If a 503 causes the alarm, the PDP may be overloaded by requests. Take appropriate action to reduce the load on the PDP by following some or all of these recommendations: 1) consider adding more PDPs and provisioning Unified CM with additional call intercept profiles and call intercept trigger points in the various configuration pages under the Call Routing menu in Cisco Unified CM Administration; 2) provision a pair of policy servers per call-intercept profile to enable load balancing; or 3) verify that the PDP server in your deployment meets or exceed the hardware requirements specified in the documentation for Cisco Enterprise Policy Manager (CEPM) or the third-party PDP solution you have deployed. If a 505 response causes the alarm, check to be sure that the PDP supports HTTP version 1.1.

FailedToReadConfig

Service Manager failed to read configuration file.

Facility/Sub-Facility

CCM_SERVICEMANAGER-GENERIC

Cisco Unified Serviceability Alarm Definition Catalog

System/Service Manager

Severity

Error (3)

Parameters

File Name(String)

Reason(String)

Recommended Action

None

FirewallMappingFailure

Firewall unreachable.

This alarm indicates that Unified CM was unable to contact the firewall in order to make a IME call. As a consequence, outbound calls are being sent over the PSTN, and inbound calls may be routed over the PSTN by your partner enterprises.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Recommended Action

Check to see that your firewall is up. Make sure the mapping service is enabled. Check that the IP address and port on the firewall for that mapping service match the configuration in Unified CM Administration. Check general IP connectivity between Unified CM and the firewall.

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

IP address(String)

Port number(UInt)

ICTCallThrottlingStart

Cisco CallManager stops handling calls for the indicated H.323 device due to heavy traffic or a route loop over the H.323 trunk.

Cisco Unified Communications Manager has detected a route loop over the H.323 trunk indicated in this alarm. As a result, Unified CM has temporarily stopped accepting calls for the indicated H.323 trunk. It's also possible that a high volume of calls are occurring over the intercluster trunk, which has triggered throttling.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error (3)

Parameters

Device Name [String] IP Address [String] Device type. [Optional] [Enum]Device description [Optional]. [String]

Enum Definitions for DeviceType

125—TRUNK

Recommended Action

In Real-Time Monitoring Tool, check the CallsActive and CallsInProgress counters for unusual activity on the indicated H.323 trunk. If the CallsActive count is significantly higher than usual, a traffic load issue may be occurring where the demand to send calls over the trunk is greater than the trunk's capacity. Monitor the situation and collect existing trace files. If the ICTCallThrottlingEnd alarm is not issued in a reasonable amount of time as deemed by your organization, contact TAC and supply the trace information you have collected. For a routing loop condition, the CallsInProgress counter will be significantly higher than usual. By examining trace files and CDR data for calls that occurred over the indicated trunk, you may be able to detect a translation pattern, route list or other routing mechanism that is part of the loop. Update the routing mechanism that resulted in the loop (generally the same number is configured on both near end and far end devices) and then reset the affected route list in an attempt to clear the route loop and if that fails, reset the affected trunk.

IDSEngineCritical

This alarm does not compromise data or prevent the use of the system but need to be monitored by the Administrator.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Changed severity level to Error from Critical.

Facility/Sub-Facility

CCM_DB_LAYER-DB

Cisco Unified Serviceability Alarm Definition Catalog

System/DB

Severity

Error (3)

Parameters

Event Class ID [String] Event class message [String] Event Specific Message [String]

Recommended Action

This alarm needs monitoring by the db admin.

IDSEngineFailure

Combined alarm for emergency and error situations. Something unexpected occurred that might compromise data or access to data or cause IDS to fail. This alarm indicates combined alarm for emergency and error situations. Something unexpected occurred that might compromise data or access to data or cause IDS to fail

Facility/Sub-Facility

CCM_DB_LAYER-DB

Cisco Unified Serviceability Alarm Definition Catalog

System/DB

Severity

Error (3)

Parameters

Event Class ID [String] Event class message [String] Event Specific Message [String]

Recommended Action

Requires Database Admin. intervention

IDSReplicationFailure

Combined alarm for emergency and error situations. IDS Replication has failed.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Route Listing element Data Collector changed to Alert Manager and existing parameters added.

Facility/Sub-Facility

DB

Cisco Unified Serviceability Alarm Definition Catalog

System/DB

Severity

Error (3)

Routing List

SDI

Event Log

Sys Log

Alert Manager

Parameters

Event Class ID [String]

Event class message [String]

Event Specific Message [String]

Recommended Action

Requires Database Admin. intervention.

ILSTLSAuthenticationFailed

Table 58: Configuration for the ILSTLSAuthenticationFailed 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 E-mail	Selected
Trigger Alert Action	Default

InsufficientFallbackIdentifiers

Cannot allocate fallback identifier.

This alarm is generated when Unified CM is processing a IME call, and is attempting to allocate a PSTN fallback DID and a DTMF digit sequence to associate with this call. However, there are too many IME calls currently in progress which are utilizing this same fallback DID, and as a result, there are no more DTMF digit sequences which could be allocated to this call. As such, this call will proceed, however mid-call fallback will not be possible for this call.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Event Log

Alert Manager

Parameter(s)

Fallback profile name(String)

Fallback E.164 number(UInt)

Current number of DTMF digits(UInt)

E.164 called party number(String)

Recommended Action

Your first course of action should be to identify the fallback profile associated with this call. Its name will be present in the alarm. Check that profile from the admin interface, and examine the current setting for “Fallback Number of Correlation DTMF Digits”. Increase that value by one, and check if that eliminates these alarms. In general, this parameter should be large enough such that the number of simultaneous IME calls made to enrolled numbers associated with that profile is always substantially less than 10 raised to the power of this

number. “Substantially” should be at least a factor of ten. For example, if you always have less than 10,000 simultaneous IME calls for the patterns associated with this fallback profile, setting this value to 5 (10 to the power of 5 is 100,000) will give you plenty of headroom and you will not see this alarm.

However, increasing this value also results in a small increase in the amount of time it takes to perform the fallback. As such, it should not be set arbitrarily large; it should be set just large enough to keep clear of this alarm. Another alternative to increasing this parameter is to add another fallback profile with a different fallback DID, and associate that fallback profile with a smaller number of enrolled DID patterns. This will allow you to get by with a smaller number of digits.

InvalidIPNetPattern

An invalid IP address is configured in one or more SIP route patterns in Cisco Unified CM Administration.

Facility/Sub-Facility

CCM_CALLMANAGER/CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error (3)

Parameters

Description(String)

IPAddress(String)

DeviceName(String)

Recommended Action

In Cisco Unified CM Administration, verify that the route pattern associated with the device that is identified in this alarm has an accurate and working IP address. You can learn more how to ensure that the IP address is valid by reviewing RFC 2373.

InvalidPortHandle

The handle for the opened serial port is invalid.

CMI cannot read/write to the serial port because the serial port returned an invalid handle value to CMI. The serial port may have returned an invalid handle because the system did not properly detect the USB cable.

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kInvalidPortHandle.

Cisco Unified Serviceability Alarm Definition Catalog

CMIAlarmCatalog/CMI

Severity

ERROR

Routing List

Event Log

SDI

Parameter(s)

Error Information(String)

Recommended Action

Make sure that the cable connecting the USB0 port and voice messaging system is firmly connected.

IPMAApplicationError

IPMA Facility/Sub-Facility error.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Servlet Name [String] Reason [String]

Recommended Action

See application logs for details

IPMAOverloaded

IPMA Facility/Sub-Facility overloaded.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Servlet Name [String] Reason [String]

Recommended Action

See application logs for details

IPMAFilteringDown

IPMA application filtering is down.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Servlet Name [String] Reason [String]

Recommended Action

Restart Cisco IP Manager Assistant Service.

IPv6InterfaceNotInstalled

IPv6 network interface is not installed. IPv6 option is enabled for TFTP service but the IPv6 network interface/address has not been configured on the system. Until the IPv6 network is functioning, devices that have been configured with IPv6-only will not be able to register. Devices that have been configured to use either IPv6 or IPv4 will register using IPv4. When the IPv6 network is online, IPv6-capable devices that have registered as IPv4 will remain IPv4 until they are reset, at which time they will use IPv6 if available.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Added to CallManager Catalog.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Error (3)

Parameters

None

Recommended Action

Install IPv6 network interface and then restart TFTP service.

kANNDeviceRecordNotFound

ANN device record not found. A device record for the announcer device was not found in the database. The ANN device is normally automatically added when the server is added to the database.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Warning to Error.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error

Recommended Action

To add the ANN device to database you will need to remove/delete the server and read the server. WARNING: This may result in having to manually reconfigure many different settings such as Media Resource Groups, CallManager Groups and many others.

kCFBDeviceRecordNotFound

CFB device record not found. A device record for the conference bridge device was not found in the database. The CFB device is normally automatically added when the server is added to the database.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). The severity changed from Informational to Error.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error

Recommended Action

To add the CFB device to database you will need to remove/delete the server and read the server.

Warning This may result in having to manually reconfigure many different settings such as Media Resource Groups, CallManager Groups and many others.

kCreateAudioSourcesFailed

Creating audio source class failed. Unable to create audio source subcomponent to provide audio for streaming. This may be due to lack of memory.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1) Following parameters added: • OS Error Code(Int) • OS Error Description(String)

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error (3)

Parameters

OS Error Code(Int)

OS Error Description(String)

Recommended Action

Restart the Cisco IP Voice Media Streaming App service or restart the server.

kCreateControlFailed

Stream Control create failure. Create stream control subcomponent. The error may be due to lack of memory.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.

Cisco Unified CommunicationsRelease	Action
8.0(1)	This alarm is available in 8.0(1) Following parameters added: • OS Error Code(Int) • OS Error Description(String)

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error (3)

Parameters

Codec Type [String]

OS Error Code [Int]

OS Error Description [String]

Recommended Action

Reset the MOH device. If continues to fail restart the Cisco IP Voice Media Streaming App service or restart the server.

kDbConnectionFailed

Database connection failed.

Facility/Sub-Facility

CCM_DB_LAYER-DB

Cisco Unified Serviceability Alarm Definition Catalog

System/DB

Severity

Error (3)

Parameters

Additional Information [String]

Recommended Action

Enable trace for the database layer monitor to get specific error information.

kIPVMSDeviceDriverNotFound

Cisco IP voice media streaming driver not found. The Cisco IP voice media streaming driver was not found or is not installed. The Cisco IP Voice Media Streaming App service cannot run until this error is resolved. All software media devices (ANN, CFB, MOH, MTP) for this server will not be available.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1).

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error (3)

Recommended Action

Check the system log for an error when the system attempted to load IpVms driver at the last server startup. A server restart is required to cause the driver to be loaded.

kIpVmsMgrNoLocalHostName

Unable to retrieve the local host server name. The Cisco IP Voice Media Streaming App service will terminate. No software media devices (ANN, CFB, MOH, MTP) will be available while the service is stopped.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1).

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error (3)

Recommended Action

Check the configuration settings for the server name, DHCP, or DNS. Monitor the status of Cisco IP Voice Media Streaming App service. The service will not operate without a valid server name.

kIpVmsMgrNoLocalNetworkIPAddr

Unable to retrieve the network IP address for host server. Unable to obtain the network IP (dotted) address. The Cisco IP Voice Media Streaming App service will terminate. The software media devices (ANN, CFB, MOH, MTP) will be unavailable while this service is stopped.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1).

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error (3)

Recommended Action

Monitor the status of the Cisco IP Voice Media Streaming App service. It should be automatically restarted. If the error occurs again, check the server IP configuration (DHCP, IP address).

kIPVMSMgrWrongDriverVersion

Wrong version of device driver. An incompatible device driver was found. The Cisco IP Voice Media Streaming App service will terminate. The software media devices (ANN, CFB, MOH, MTP) will be unavailable while the service is stopped.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Following parameters are removed: • Found [ULong] • Need [ULong]

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error (3)

Recommended Action

Restart the server to ensure the most recent driver is started. If the error continues, then reinstall Cisco Unified Communications Manager to get the proper driver version installed.

kMOHTFTPGoRequestFailed

Transfer of MOH source file to working path failed. An error was encountered when trying to copy or update a Music-on-Hold audio source file.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Following parameters added: Error Description [String] Source Path [String] Destination Path [String] OS Error Code [Int] OS Error Description [String]

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error (3)

Parameters

Error Description [String] File Name [String] Source Path [String] Destination Path [String]

OS Error Code [Int] OS Error Description [String]

Recommended Action

Use the Platform CLI to verify the source path and file exist. If the file does not exist then use Cisco Unified CM Admin to reupload the missing audio source to this specific server. Reinstall the Cisco Unified Communications Manager to have all required paths created.

kPWavMgrThreadxFailed

WAV playing manager thread creation failed. The process component used for playing WAV files failed to start, possibly due to low system resources.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error (3)

Parameters

OS Error Description(String)

Recommended Action

Restart the Cisco IP Voice Media Streaming App service or restart server.

kReadCfgUserLocaleEnterpriseSvcParm

Error reading Enterprise User Locale configuration. A database exception was encountered when reading the default Enterprise User Locale setting. Default of US English will be used.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error (3)

Recommended Action

Verify that the Enterprise parameter setting for User Locale is configured using the CCM Admin web page. Restart the Cisco IP Voice Media Streaming App service.

kRequestedANNStreamsFailed

The requested resources for the configured number of annunciator calls (Call Count service parameter) was not available. If the value gets shown as “Allocated,” it is non-zero.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Added descriptive text and Recommended Actions. Following parameters are removed: Requested streams [ULong] Allocated streams [ULong]

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error (3)

Recommended Action

Verify that the ANN Call Count service parameter is correct. A server restart may be needed to recover resources.

LostConnectionToSAFForwarder

Connection to the SAF Forwarder has been lost.

A TCP connection failure caused the connection between the SAF Forwarder and Unified CM to be lost. When the TCP connection is restored, Unified CM attempts to connect to the SAF Forwarder automatically. If IP connectivity is unreachable for longer than the duration of the Cisco CallManager service parameter CCD Learned Pattern IP Reachable Duration, calls to learned patterns will be routed through the PSTN instead. Calls through the PSTN to learned patterns will be maintained for a certain period of time before the PSTN failover times out.

Cisco Unified Serviceability Alarm Catalog

CallManager/CallManager

Severity

Error

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameters

IP Address(String)

SafClientHandle(UInt)

Recommended Action

Investigate possible causes of a TCP connection failure, such as power failure, loose cables, incorrect switch configuration, and so on, and correct any issues that you find. After the connection is restored, CCD will try to register/sync with the SAF Forwarder automatically.

MultipleSIPTrunksToSamePeerAndLocalPort

Multiple trunks have been configured to the same destination and local port, which resulted in a conflict. Only one trunk is allowed for one destination/local port combination. The latest trunk invalidated earlier.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error

Parameters

Peer IP Address. [String] Local IP Port [UInt] Old Device name. [String] Old Device Instance. [String] New Device name. [String] New Device Instance. [String]

Recommended Action

Check the SIP Trunk Configuration in Cisco Unified CallManager Administration and verify that only one SIP trunk has been configured to the same destination address and local port.

NodeNotTrusted

Untrusted Node was contacted. Application could not establish secure connection (SSL handshake failure) with another application. It could be due to certificate for tomcat service where the application is hosted is not trusted (not present in the keystore).

Cisco Unified Serviceability Alarm Definition Catalog

System/EMAlarmCatalog

Severity

ERROR

Routing List

Sys Log

Event Log

Alert Manager

Parameter(s)

Date/Time(String)

Hostname/Ip Address(String)

Recommended Action

1. Ensure that "tomcat-trust" keystore on each CCM node contains the tomcat certificates for every other node within a cluster (Logon to **OS Administration Page** > **Security** > **Certificate Management** > **Check the certificates in tomcat-trust**).
2. If EMCC is enabled, then ensure that a bundle of all tomcat certificates (PKCS12) has been imported into the local tomcat-trust keystore (Logon to **OS Administration Page** > **Security** > **Certificate Management** > **Look for certificates in tomcat-trust**).

NumDevRegExceeded

The allowed number of registered devices was exceeded.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error (3)

Parameters

Maximum Devices [Int]

Recommended Action

If you did not expect to exceed the number of devices and you have auto-registration enabled, go to **Device** > **Phones** in Cisco Unified CM Administration and search for phones starting with "auto". If you see any unexpected devices which may not belong in the system (such as intruder devices) locate that device using the IP address and remove it from the system. Or, if your licenses and system resources allow, increase the value in the Cisco CallManager service parameter, Maximum Number of Registered Devices.

PublishFailedOverQuota

Each IME server has a fixed quota on the total number of DIDs it can write into the IME distributed cache. When this alarm is generated, it means that, even though you should be under quota, due to an extremely unlikely statistical anomaly, the IME distributed cache rejected your publication, believing you were over quota. You should only see this alarm if you are near, but below, your quota. This error is likely to be persistent, so that the corresponding E.164 number from the alarm will not be published into the IME distributed cache. This means that you will not receive VoIP calls towards that number - they will remain over the PSTN.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	New Alarm for this release.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR_ALARM

Recommended Action

The alarm will include the name of the IME server, and the current and target quota values. The first thing to check is to make sure that you have correctly provisioned the right set of DID prefixes on all of the Unified CM clusters sharing that same IME server on the same IME distributed cache. If that is correct, it means you have exceeded the capacity of your IME server, and you require another. Once you have another, you can now split your DID prefixes across two different IME client instances, each on a different IME server. That will alleviate the quota problem.

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

The DID for which the Publish was attempted(String)

Server name(String)

Current quota(UInt)

Maximum target quota(UInt)

ReadConfigurationUnknownException

An exception is caught while retrieving enterprise parameters value from database at TFTP service startup. This is usually caused by a failure to access the Cisco Unified Communications Manager database.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kReadConfigurationUnknownException.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Error (3)

Recommended Action

In Cisco Unified Serviceability, enable Detailed level traces in the Trace Configuration window for TFTP and Cisco Database Layer Monitor services. Also, use RTMT to look for errors that may have occurred around the time of the alarm.

RsvpNoMoreResourcesAvailable

RSVP Agent resource allocation failed.

The alarm occurs when allocation of an RSVP Agent fails for all the registered RSVP Agents (RSVP Agents are basically MTPs or transcoder devices which provide RSVP functionalities) belonging to the Media Resource Group List and Default List. Each RSVP Agent may fail for different reasons. Following are some of the reasons that could cause an RSVP Agent allocation to fail: available MTP/transcoders do not support RSVP functionality; a capability mismatch between the device endpoint and MTP/transcoder, codec mismatch between the endpoint and the MTP/transcoder; a lack of available bandwidth between the endpoint and the MTP/transcoder; or because the MTP/transcoder resources are already in use.

A capability mismatch may be due to the MTP/transcoder not supporting one or more of the required capabilities for the call such as Transfer Relay Point (which is needed for QoS or firewall traversal), RFC 2833 DTMF (which is necessary when one side of the call does not support RFC 2833 format for transmitting DTMF digits and the other side must receive the DTMF digits in RFC2833 format, resulting in conversion of the DTMF digits), RFC 2833 DTMF passthrough (in this case, the MTP or transcoder does not need to convert the DTMF digits from one format to another format but it needs to receive DTMF digits from one endpoint and transmit them to the other endpoint without performing any modifications), passthrough (where no codec conversion will occur, meaning the media device will receive media streams in any codec format and transmit them to

the other side without performing any codec conversion), IPv4 to IPv6 conversion (when one side of the call supports only IPv4 and the other side of the call supports only IPv6 and so MTP needs to be inserted to perform the necessary conversion between IPv4 and IPv6 packets), or multimedia capability (if a call involving video and/or data in addition to audio requires insertion of an MTP or transcoder then the MTP/transcoder which supports multimedia will be inserted).

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Media Resource List Name(String) parameter is added.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error (3)

Parameter(s)

Media Resource List Name(String)

Recommended Action

RSVP Agents are basically Cisco IOS MTPs or transcoder devices which provide RSVP functionalities. Check the user manual of the configured MTPs and transcoders to see whether they support RSVP functionality. If none of them support RSVP functionality either they need to be upgraded (if upgraded version support RSVP functionality) or additional MTP or transcoders need to be installed which support RSVP functionality. If the RSVP Agent (MTP or transcoder) allocation is failing due to a capability mismatch, it's possible that the media device does not support the requested capability (such as IPv4 to IPv6 conversion, passthrough) or the capability might not be configured in the device. Please check the user guide and documentation of the media device to make sure that device supports all the necessary capabilities.

Also, caution should be taken care if all the MTP or transcoders are configured with all the supported capabilities. There are certain capabilities (such as RFC 2833 DTMF or RFC 2833 DTMF passthrough or passthrough) which could be supported by most of the MTPs or transcoders and there may be certain capabilities (such as IPv4 to IPv6 conversion and vice versa or RSVP Agent functionality or Transfer Relay Point or multimedia capability) which can be supported by only by a single MTP or transcoder depending on the devices that you have.

For example, you may have end devices belonging to different locations and may need to reserve the bandwidth only between two locations; calls between other locations may not need to reserve the bandwidth. Now, suppose all the MTPs or transcoders are configured with all the supported capabilities and only one MTP/transcoder supports RSVP functionality; if this MTP/transcoder is configured with all the supported capabilities (which all the other MTPs or transcoders in the same MRGL or default MRGL also support) it may happen that this MTP can get allocated for Transfer Relay Point or RFC 2833 DTMF or RFC 2833 DTMF

passthrough or passthrough instead. As a result, when a need arises to reserve the bandwidth (which other MTPs or transcoders in the same MRGL or default MRGL do not support), all the resources of this MTP/transcoder may be in use and the RSVP Agent allocation may fail.

To avoid this situation, set the priority of the media resources appropriately. This can be done only in the Media Resource Group List and not in the Default List of the media resources. In any Media Resource Group List all the Media Resource Groups have different priorities and during allocation the first Media Resource Group is checked for availability of the requested type of the media devices. The first Media Resource Group in the Media Resource Group List will have the highest priority, then the second one and so on. To check all the Media Resource Groups and their priority go the Media Resources and Media Resource Group List of Cisco Unified CM Administration page and click the appropriate Media Resource Group List and check the Selected Media Resource Groups; the priority decreases from top to bottom. Position the MTP or transcoder that you want to be selected for the basic functionalities in the higher priority Media Resource Groups whereas the ones with more rare functionality can be positioned in the Media Resource Groups with lower priority. RSVP Agent allocation may fail due to codec mismatch between the end point and the RSVP Agent or MTP/transcoder.

A solution may be to configure the MTP/transcoder with all the supported codecs (as specified in the user guide of the MTP/transcoder), but be aware that doing so might result in too much bandwidth being allocated for calls. You'll need to weigh different factors such as the total amount of available bandwidth, the average number of calls, approximate bandwidth use per call (not involving MTP/transcoder), and so on, and accordingly calculate the maximum bandwidth that can be allocated per call involving an MTP/transcoder and take that into consideration when configuring the supported codecs in the MTPs and transcoders. A good idea is to configure the media devices with all the supported codecs and set the region bandwidths to restrict too much bandwidth usage (refer to the Unified CM documentation for details on region and location settings).

Also, there may be codec mismatch between the endpoint and the MTP/transcoders after considering the region bandwidth between the MTP/transcoder and the endpoint. Increasing the region bandwidth may be a solution to the problem, but that decision should be made after careful consideration of the amount of bandwidth you're willing to allocate per call between the set of regions.

Another possible cause that an MTP/transcoder did not get allocated is because there was not enough available bandwidth for the call. This can happen if the MTP/transcoder and endpoint belong to different locations and the bandwidth that is set between the locations is already in use by other calls. Examine the bandwidth requirements in your deployment to determine whether bandwidth between the locations can be increased. However, note that increasing the bandwidth between these two locations means that you may need to reduce the bandwidth between other locations.

Refer to the System Guide, SRNDs, and related Unified CM documentation for more details. Be aware that reducing the bandwidth or removing the higher bandwidth codecs from configuration may result in poor voice quality during call. Consider increasing the total amount of network bandwidth. Finally, if RSVP Agent allocation fails due to MTP/transcoder not supporting RSVP functionality or capability mismatch or all the resources being in use, consider installing additional MTP or transcoder devices which support RSVP functionality.

RTMT_ALERT

A Real-Time Monitoring Tool (RTMT) process in the AMC service uses the alarm mechanism to facilitate delivery of RTMT alerts in the RTMT AlertCentral or through email.

Cisco Unified Serviceability Alarm Definition Catalog

System/RTMT

Severity

ERROR

Routing List

Event Log

Sys Log

Parameter(s)

Name(String)

Detail(String)

Recommended Action

Check AlertCentral in RTMT or any alerts that you have received through email to determine what issue has occurred and learn the recommended actions to resolve it. In AlertCentral, right-click the alert to open the alert information.

RTMT-ERROR-ALERT

This alert is generated by RTMT AlertMgr. See Alert Detail for explanation.

Facility/Sub-Facility

CCM_RTMT-RTMT

Cisco Unified Serviceability Alarm Definition Catalog

System/RTMT

Severity

Error (3)

Parameters

Name [String] Detail [String]

Recommended Action

See Alert Detail for more information.

SAFForwarderError

SAF Forwarder error response sent to Unified CM.

Cisco Unified Serviceability Alarm Catalog

CallManager/CallManager

Severity

Error

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameters

IP Address(String)

SafClientHandle(UInt)

Application User Name(String)

Reason Code and Description(Enum)

SAF Protocol Version Number(String)

Service ID(UInt)

Sub Service ID(UInt)

Recommended Action

Refer to the reason code and description (help text) for specific information and actions (where applicable) for this alarm.

Related Topics

Reason Code Enum Definitions for SAFForwardError, on page 207

Reason Code Enum Definitions for SAFForwardError

Value	Definition
400	SAF_BAD_REQUEST - SAF Forwarder was unable to accept the request due to incorrect syntax (malformed), missing required attributes, and other similar reasons. Investigate the configuration between the SAF Forwarder and Unified CM to be certain that all settings are correct for your deployment. In particular, check the Client Label configured on the router to make certain that it matches the Client Label configured in Cisco Unified CM Administration on the SAF Forwarder Configuration window (**SAF** > **SAF Forwarder**).

Value	Definition
431	SAF_INTEGRITY_CHECK_FAILURE - A message failed to pass SAF Forwarder security validation. This can occur because of misconfiguration, a potential attack, or more commonly by incorrect provisioning of the password on the Forwarder and SAF client. Reprovision the password and keep a watch on further SAF INTEGRITY CHECK FAILURE alarms. If you receive a persistent number of SAF INTEGRITY CHECK FAILURE alarms, close the interface between SAF Forwarder and Unified CM and investigate the source of the IP packets.
435	**INFO LEVEL** SAF_MISSING_NONCE - A nonce (a random parameter generated when the message is sent) is missing from the message. The system will resend with a new nonce automatically. No action is required.
436	SAF_UNKNOWN_USERNAME - Unified CM sent the SAF Forwarder an Application User name that is not configured on the router or that does not match the router's configuration. Check the Application User Name on the router and in the Application User Configuration window in Cisco Unified CM Administration to be sure they match.
438	**INFO LEVEL** SAF_STALE_NONCE - A nonce (a random parameter generated when the message is sent) has aged out (gone stale). The system will resend with a new nonce automatically. No action is required.
471	**INFO LEVEL** SAF_BAD_CLIENT_HANDLE - SAF_BAD_CLIENT_HANDLE - Unified CM sent the SAF Forwarder a Register message (for KeepAlive purposes) or unregister message with the mandatory CLIENT_HANDLE value, but the SAF Forwarder did not recognize the client handle. Unified CM will attempt to reregister with the SAF Forwarder without a client handle. This alarm is for informational purposes only; no action is required.
472	**INFO LEVEL** SAF_VERSION_NUMBER_TOO_LOW - Unified CM published a service (such as Hosted DN) whose version number is now lower than when it was previously published to the SAF Forwarder. The service is out of sync with the SAF Forwarder. Unified CM will republish the service in an attempt to resynch with the SAF Forwarder. This alarm is for informational purposes only; no action is required.
473	**INFO LEVEL** SAF_UNKNOWN_SERVICE - Unified CM attempted to unpublish a service from the SAF network but the SAF Forwarder does not have a publish record for that service. This alarm is for informational purposes only; no action is required.
474	**INFO LEVEL** SAF_UNREGISTERED - Unified CM attempted to publish or subscribe to the SAF Forwarder, but Unified CM is not registered with SAF Forwarder. Unified CM will automatically reregister with the SAF Forwarder before attempting to publish or subscribe. This alarm is for informational purposes only; no action is required.
475	**INFO LEVEL** SAF_BAD_FILTER - Unified CM attempted to subscribe to the SAF Forwarder with a filter that does not match any of the SAF Forwarder's current filters. Unified CM will resend the subscribe message with the appropriate filter value. This alarm is for informational purposes only; no action is required.

Value	Definition
476	SAF_UNKNOWN_SUBSCRIPTION - Unified CM sent a subscribe or unsubscribe message to the SAF Forwarder but the message contained a Service ID that was not familiar to the SAF Forwarder. Without a recognized Service ID, Unified CM cannot subscribe to the SAF Forwarder. Recommended action is to contact the Cisco Technical Assistance Center (TAC).
477	**INFO LEVEL** SAF_ALREADY_REGISTERED - Unified CM attempted to register with the SAF Forwarder but SAF Forwarder indicates that Unified CM is already registered. Unified CM will close and reopen the TCP connection and send a new register request without a client handle to SAF Forwarder. This alarm is for informational purposes only; no action is required.
478	SAF_UNSUPPORTED_PROTOCOL_VERSION - Unified CM attempted to register with the SAF Forwarder using a SAF protocol version number that is greater than the protocol version number supported by the SAF Forwarder. Issue a show version command on the SAF Forwarder CLI to determine the SAF Forwarder protocol version; refer to the information in this alarm for the SAF protocol version number. If the versions do not match, check the Cisco Unified Communications Manager Software Compatibility Matrix (available on Cisco.com) to determine whether the SAF protocol version number that is in use on this Unified CM is compatible with the SAF Forwarder protocol version. If it is not, upgrade the lower-versioned component so that both Unified CM and the SAF Forwarder use the same, compatible version.
479	SAF_UNKNOWN_AS - Unified CM attempted to register to the SAF Forwarder but the registration message contained a Client Label that was not familiar to the Autonomous System (AS) on the SAF Forwarder router. Recommended action is to issue the appropriate CLI commands on the SAF Forwarder to associate the Client Label with the autonomous system on the router (refer to the Configuration Guide for the router) and configure the same Client Label in the Client Label field on the SAF Forwarder Configuration window in Cisco Unified CM Administration and click Save. When the Client Label is saved in Cisco Unified CM Administration, Unified CM automatically sends a new registration request to the SAF Forwarder with the updated Client Label information.
500	**INFO LEVEL** SAF_RESPONDER_ERROR - Unified CM sent a message (such as register/unregister/publish/unpublish/subscribe) to the SAF Forwarder but the SAF Forwarder responded that it is unable to process the message at this time. This might be due to heavy message queuing, internal resource issues, and so on. Unified CM will wait several seconds and then retry the request. This alarm is for informational purposes only; no action is required.
1000	SAF_INVALID_CONNECTION_DETAILS

SAFResponderError

SAF Responder Error 500.

This is raised when SAF forwarder doesn't know the transaction ID within SAF response from this Cisco Unified CM.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameter(s)

Client Handle(String)

Service Id(UInt)

Sub Service ID(UInt)

Instance ID1(UInt)

Instance ID2(UInt)

Instance ID3(UInt)

Instance ID4(UInt)

Recommended Action

No action is required.

ScheduledCollectionError

An error occurred while executing scheduled collection.

Facility/Sub-Facility

CCM_TCT-LPMTCT

Cisco Unified Serviceability Alarm Definition Catalog

System/LpmTct

Severity

Error (3)

Parameters

JobID [String] Reason [String]

Recommended Action

Review configuration for scheduled collection job under Job Status window.

SerialPortGetStatusError

When CMI tries to get the status of serial port, the operating system returns an error.

CMI triggers this alarm when it cannot get the status of the serial port. An inability to receive the serial port status information can be caused by a loose or disconnected USB cable.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kSerialPortGetStatusError.

Cisco Unified Serviceability Alarm Definition Catalog

CMIAlarmCatalog/CMI

Severity

ERROR

Routing List

Event Log

SDI

Parameter(s)

Serial Port Getting Status Error(String)

Recommended Action

Make sure that the cable connecting the USB0 port and voice messaging system is firmly connected.

SerialPortSetStatusError

When CMI tries to set the status of serial port, the operating system returns an error.

CMI triggers this alarm when it cannot set the status of the serial port. An inability to receive the serial port status information can be caused by a loose or disconnected USB cable.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kSerialPortSetStatusError.

Cisco Unified Serviceability Alarm Definition Catalog

CMIAlarmCatalog/CMI

Severity

ERROR

Routing List

Event Log

SDI

Parameter(s)

Serial Port Setting Status Error(String)

Recommended Action

Make sure that the cable connecting the USB0 port and voice messaging system is firmly connected.

ServiceActivationFailed

Failed to activate a service.

Facility/Sub-Facility

CCM_SERVICEMANAGER-GENERIC

Cisco Unified Serviceability Alarm Definition Catalog

System/Service Manager

Severity

Error (3)

Parameters

Service Name(String)

Reason(String)

Recommended Action

None

ServiceDeactivationFailed

Failed to deactivate a service.

Facility/Sub-Facility

CCM_SERVICEMANAGER-GENERIC

Cisco Unified Serviceability Alarm Definition Catalog

System/Service Manager

Severity

Error (3)

Parameters

Service Name(String)

Reason(String)

Recommended Action

None

ServiceFailed

Service terminated.

Facility/Sub-Facility

CCM_SERVICEMANAGER-GENERIC

Cisco Unified Serviceability Alarm Definition Catalog

System/Service Manager

Severity

Error (3)

Parameters

Service Name(String)

Process ID(Int)

Recommended Action

None

ServiceStartFailed

Failed to start service.

Facility/Sub-Facility

CCM_SERVICEMANAGER-GENERIC

Cisco Unified Serviceability Alarm Definition Catalog

System/Service Manager

Severity

Error (3)

Parameters

Service Name(String)

Reason(String)

Recommended Action

None

ServiceStopFailed

Failed to stop service.

Facility/Sub-Facility

CCM_SERVICEMANAGER-GENERIC

Cisco Unified Serviceability Alarm Definition Catalog

System/Service Manager

Severity

Error (3)

Parameters

Service Name(String)

Reason(String)

Recommended Action

None

ServiceExceededMaxRestarts

Service exceeded maximum allowed restarts.

Facility/Sub-Facility

CCM_SERVICEMANAGER-GENERIC

Cisco Unified Serviceability Alarm Definition Catalog

System/Service Manager

Severity

Error (3)

Parameters

Service Name(String)

Reason(Int)

Recommended Action

If service is required to be running, restart it.

SIPNormalizationResourceWarning

The normalization script has exceeded an internal resource threshold.

The normalization script for the indicated SIP device has exceeded an internal threshold for resource consumption. This alarm can occur for memory consumption, or when the script is close to exceeding the configured allowance of Lua instructions. When the amount of memory (as defined in the Memory Threshold field) or the number of Lua instructions utilized by this script (as defined by the Lua Instruction Threshold) exceeds an internal threshold, this alarm is triggered.

Examples

1. If the memory threshold is set to 100 KB and the internal threshold is 80%, this alarm will occur when this script has consumed 80 KB of memory. The internal threshold is not configurable and may fluctuate from Cisco Unified CM release to release.
2. If the Lua Instruction Threshold is set to 2000 and the internal threshold is 50%, this alarm will occur when the script has executed 1000 Lua instructions.

This alarm warns that the resources (either memory or Lua instructions) have crossed an internal mark, where investigation into the consumption of those resources may be advisable to ensure the health of the script.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	• New alarm for this release.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error

Routing List

SDI

Sys Log

Event Log

Parameters

Device Name(String)

Script Name(String)

Script Function(String)

Script Type(String)

Reason Code(Enum)

Reason Text(String)

In Use Memory(UInt)

Memory Threshold (UInt)

In Use Lua Instructions(UInt)

Lua Instruction Threshold(UInt)

Recommended Action

1 Examine the thresholds (Memory Threshold and Lua Instruction Threshold) configured in the SIP Normalization Script Configuration window.

2 Evaluate if the thresholds can be increased (take into consideration the CPU resources and memory when deciding to increase these values), or examine the script to determine if the message handlers can be written more efficiently to reduce the number of instructions in the script.

3 Examine the script for logic errors. If the script is functioning normally but contains extensive logic, consider increasing the value in the Lua Instruction Threshold field. Be aware that more computing resources will be consumed as a result. You can also examine SDI trace files for additional details about this resource condition. For scripts provided by Cisco, contact the Cisco Technical Assistance Center (TAC).

4 Investigate and correct the resource issue before the script closes. When the values that have been configured in the Memory Threshold field, or Lua Instruction Threshold field or both the fields on the SIP Normalization Script Configuration window are met, the script closes and the SIPNormalizationScriptClosed alarm also occurs. For additional information when troubleshooting, check the SIP Normalization counter, MemoryUsagePercentage to learn the current resource usage.

Related Topics

Reason Code Enum Definitions for SIPNormalizationResourceWarning, on page 217

Reason Code Enum Definitions for SIPNormalizationResourceWarning

Value	Definition
1	InternalLuaInstructionsThreshold—The script exceeds the internal threshold for the number of Lua instructions.
2	InternalMemoryThreshold—The script exceeds the internal threshold for script memory usage.

SIPNormalizationScriptError

Description

A script error occurred.

Explanation

Cisco Unified CM encountered an error during loading, initializing, or during execution of the SIP normalization script for the indicated SIP device. If the error was due to a resource issue, the SIPNormalizationResourceWarning alarm will also be issued. The Configured Action shown in this alarm may differ from the Resulting Action shown in this alarm because certain errors, such as those occurring during loading or initialization, cannot be configured. If the script closes three times within a 10 minute window due to errors, Cisco Unified CM will follow the configured action three times; on the fourth occurrence of the error, Unified CM disables the script and issues the SIPNormalizationAutoResetDisabled alarm.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	• New alarm for this release.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

Device Name(String)

Script Name(String)

Script Function(String)

Script Type(String)

Error Code(Enum)

Error Code Text(String)

Error Message(String)

Configured Action(String)

Resulting Action(String)

In Use Memory(UInt)

Memory Threshold(UInt)

In Use Lua Instructions(UInt)

Lua Instruction Threshold(UInt)

Recommended Action

1 Examine SDI trace files for details regarding the error such as function calls and the call ID. This will help you to troubleshoot the error.

Examine the script for syntax or logic errors; for scripts provided by Cisco, contact the Cisco Technical Assistance Center (TAC). If the error was due to a resource issue, the SIPNormalizationResourceWarning alarm will also be issued. Check the SIPNormalizationResourceWarning alarm for additional information and recommended actions.

Related Topics

Reason Code Enum Definitions SIPNormalizationScriptError, on page 219

Reason Code Enum Definitions SIPNormalizationScriptError

Value	Definition
1	LoadError —The script failed to load either due to a syntax error in the script or a resource error; check the Recommended Actions for instructions.
2	InitializationError—The script encountered a failure while initializing either due to a syntax error in the script or a resource error; check the Recommended Actions for instructions.
3	ExecutionError—The script encountered a failure during execution; check the Recommended Actions for instructions.
4	InternalError—The system encountered an unexpected condition during execution; check the Recommended Actions for instructions.

SIPTrunkOOS

All remote peers are out of service and unable to handle calls for this SIP trunk.

This alarm provides the list of unavailable remote peers, where each peer is separated by semicolon. It also provides the reason code received by the SIP trunk, in response to an Options request sent to remote peer. For each peer, the alarm provides the hostname or SRV (if configured on SIP trunk), resolved IP address, port number, and reason code in the following format:

ReasonCodeType=ReasonCode.

The ReasonCodeType depends on a SIP response from the remote peer as defined in SIP RFCs (remote), or depends on a reason code provided by Unified CM (local).

The examples of possible reason codes include:

- Remote = 503 (“503 Service Unavailable” a standard SIP RFC error code)
- Remote = 408 (“408 Request Timeout” a standard SIP RFC error code)
- Local = 0 (local SIP stack is unable to send the message due to socket send error)
- Local = 1 (request timeout)
- Local = 2 (local SIP stack is unable to create a socket connection with remote peer)
- Local = 3 (DNS query failed)

  For Local=3, IP address in the alarm is represented as zero, and when DNS SRV is configured on SIP trunk then the port is represented as zero.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	• New alarm for this release.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Error

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

SIP Trunk Name(String)

Unavailable remote peers with Reason Code(String)

Recommended Action

- For Remote = 503, the possible reasons include:
  - Route/SIP trunk for originating side does not exist on remote peer. If remote peer is Unified CM, add a new SIP trunk in Unified CM Administration for the remote peer (**Device** > **Trunk**) and ensure the Destination Address and Destination Port fields are configured to point to the originating host (the originating host is the same node on which this alarm was generated).
  - Route/SIP trunk for originating side does exist on remote peer but the port is either used for a SIP phone or a different SIP trunk. If remote peer is Unified CM, in the Unified CM Administration for the remote peer (**Device** > **Trunk**), ensure the Destination Port on the originating side is configured to be the same as the incoming port on the terminating side SIP Trunk Security Profile.
  - Remote peer has limited resources to handle new calls. If remote peer is administered by a different system administrator, communicate the resource issue with the other administrator.
- For Remote = 408, the possible reason includes:

- Remote peer has limited resources to handle new calls. If remote peer is administered by a different system administrator, communicate the resource issue with the other administrator.

- For Local = 1, the possible reason could be that no responses are received for OPTIONS request after all retries, when UDP transport is configured in the SIP trunk Security Profile assigned to the SIP trunk on the originating side.

  To fix this issue, perform the following steps:

  - If remote peer is Unified CM, in the remote peer Serviceability application, choose **Tools** > **Control Center** (Feature Services) and ensure the Cisco CallManager service is activated and started.
  - In the Unified CM Administration for the remote peer, choose **Device** > **Trunk**, and ensure the SIP trunk exists with the incoming port in associated SIP Trunk Security Profile configured to be same as originating side SIP Trunk destination port.
  - Check the network connectivity by using the CLI command utils network ping <remote peer> at the originating side.

- For Local = 2, the possible reason could be that Unified CM is unable to create the socket connection with remote peer.

  To fix this issue, perform the following steps:

  - If remote peer is Unified CM, in the remote peer Serviceability application, choose **Tools** > **Control Center** (Feature Services) and ensure the Cisco CallManager service is activated and started.
  - In the Unified CM Administration for the remote peer, choose **Device** > **Trunk** and ensure the SIP trunk exists with the incoming port in associated SIP Trunk Security Profile configured to be same as originating side SIP Trunk destination port.
  - Check the network connectivity by using the CLI command utils network ping <remote peer> at the originating side.

- For Local = 3, the possible reason could be that DNS server is not reachable, or DNS is not properly configured to resolve the hostname or SRV which is configured on the local SIP trunk.

  To fix this issue, perform the following steps:

  1. In the OS Administration, choose **Show** > **Network** and verify whether the DNS details are correct. If it is not correct, configure the correct DNS server information by using the CLI command set network dns primary.
  2. Check the network connectivity with DNS server by using the CLI command utils network ping <remote peer>, and ensure the DNS server is properly configured.

SparePartitionLowWaterMarkExceeded

The percentage of used disk space in the spare partition has exceeded the configured low water mark.

Note Spare Partition is not used for Intercompany Media Engine server. So this alert will not be triggered for Intercompany Media Engine.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.

Facility/Sub-Facility

CCM_TCT-LPMTCT

Cisco Unified Serviceability Alarm Definition Catalog

System/LpmTct

Severity

Error (3)

Parameters

UsedDiskSpace [String] MessageString [Optional]. [String]

Recommended Action

Login into RTMT and check the configured threshold value for LogPartitionLowWaterMarkExceeded alert in Alert Central. If the configured value is set to a lower than the default threshold value unintentionally, change the value to default. Also, examine the trace and log file setting for each of the application in trace configuration page under Cisco Unified CM Serviceability.

If the number of configured traces or logs is set to greater than 1000, adjust the trace settings from trace configuration page to default. Also, clean up the trace files that are less than a week old. You can clean up the traces using cli “file delete” or using Remote Browse from RTMT Trace and Log Central function.

SystemResourceError

A system call failed.

Facility/Sub-Facility

CCM_SERVICEMANAGER-GENERIC

Cisco Unified Serviceability Alarm Definition Catalog

System/Service Manager

Severity

Error (3)

Parameters

System Call(String)

Service(String)

Reason(String)

Recommended Action

None

TestAlarmError

Testing error alarm.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Test

Severity

Error (3)

Recommended Action

None

ThreadPoolProxyUnknownException

Unknown exception was caught while processing file request. This usually indicates a lack of memory when there is a system issue such as running out of resources.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kThreadPoolProxyUnknownException.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Error (3)

Recommended Action

Use RTMT to monitor the system memory resources and consumption and correct any system issues that might be contributing to a reduced amount of system resources.

UnableToOpenMohAudioSource

The Music On Hold audio source file cannot be opened. This alarm occurs when Music On Hold fails because the MOH audio source file cannot be opened. The caller will hear silence instead of the desired Music on Hold audio.

History

Cisco Unified Communications Release	Action
10.0(1)	Error message added.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Error (3)

Routing List

SDI

Sys Log

Event Log

Alert Manager

Parameters

MohAudioSourceFileName [String]

MohAudioSourceId [Int]

OS Error Code [Int]

OS Error Code Text [String]

Recommended Action

Use Cisco Unified CM Administration for “MOH Audio File Management” on this specific MOH Cisco Unified Communications Manager server to check that the Music On Hold audio source file has been uploaded to this specific server. Note that MOH audio files must be uploaded using the Cisco Unified CM Administration page of each MOH server in the cluster before that server can play the audio file. If you need to upload the file, you will need to reset this MOH device after the upload so that it will be accessible by the MOH device.

UnableToRegisterwithCallManagerService

CTI cannot communicate with Cisco CallManager service to register supplementary service features.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

ERROR

Routing List

SDL

SDI

Sys Log

Event Log

Recommended Action

Check the status of the Cisco CallManager service in **Cisco Unified Serviceability** > **Tools** > **Control Center - Featured Services**. At least one Cisco CallManager service should be running in the cluster for CTIManager to register feature managers. Restart the CTIManager service if the problem persists. If CallManager service is active, verify network connectivity between the Unified CM node that hosts CTIManager service and Unified CM node that hosts CallManager service.

UserLoginFailed

User log in failed because of bad user ID or password.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Error (3)

Parameters

UserID [String]

Recommended Action

None

WDApplicationError

WebDialer Facility/Sub-Facility error.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Servlet Name [String] Reason [String]

Recommended Action

See application logs for details

WDOverloaded

WebDialer Facility/Sub-Facility overloaded.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Error (3)

Parameters

Servlet Name [String] Reason [String]

Recommended Action

See application logs for details.

Warning-Level Alarms

The warning-level alarm is 4 and action is needed but priority of action is determined by the condition. A warning about some bad condition, which is not necessarily an error. Configuration error or an alarm that by itself does not indicate a warning but several instances of the same alarm do. Examples are:

- Configuration error
- One alarm of this level may not mean that an error has occurred but multiple of these would be considered an error

AnnunciatorNoMoreResourcesAvailable

No more Annunciator resources available.

Annunciator resource allocation failed for one or more of the following reasons: all Annunciator resources are already in use; there was a codec or capability mismatch (such as the endpoint using one type of IP addressing such as IPv6, while the Annunciator supports only IPv4) between the endpoint and the Annunciator resource; not enough bandwidth existed between the endpoint and the Annunciator.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Changed severity level from Error to Warning.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Parameter(s)

Media Resource List Name(String)

Recommended Action

If all the resources of the Annunciator are already in use, check to be sure that all the Annunciators that belong to the Media Resource Groups of the indicated Media Resource Group List and Default List are configured and registered in all the applicable Unified CM nodes of the cluster. To check the registration status go to the **Media Resources** > **Annunciator** menu and click the Find button. It will display all the Annunciators with their status, device pool, and so on.

Check the status field to see whether it is registered with Unified CM. Note that the display on the status field is not a confirmation that the device is registered to Unified CM. It may happen in a Unified CM cluster that the Publisher can only write to the Unified CM database before the Publisher goes down. Because the Subscriber may not be able to write to the database, the devices may still display registered in Unified CM Administration after they are actually unregistered. However, if the Publisher is down that should generate another alarm with higher priority than this alarm.

The Annunciator allocation can fail due to codec mismatch or capability mismatch between the endpoint and the Annunciator. If there is a codec mismatch or capability mismatch (such as the endpoint using IPv6 addressing but Annunciator supporting only IPv4), an MTP or transcoder should be allocated. So, if the MTP or transcoder is not allocated then either MediaResourceListExhausted (with Media Resource Type as Media termination point or transcoder) or MtpNoMoreResourcesAvailable alarm will be generated for the same Media Resource Group List and you should first concentrate on that.

The Annunciator allocation may even fail after checking the region bandwidth between the regions to which the held party belongs and the region to which the Annunciator belongs. Increasing the region bandwidth may be a solution to the problem, but that decision should be made after careful consideration of the amount of bandwidth you're willing to allocate per call between the set of regions. You'll need to weigh different factors such as the total amount of available bandwidth, the average number of calls, the average number of calls using the Annunciator, approximate bandwidth use per call, and so on, and accordingly calculate the region bandwidth.

Another possible cause is that the bandwidth needed for the call may not be available. This can happen if the Annunciator and endpoint belong to different locations and the bandwidth that is set between the locations is already in use by other calls. Examine the bandwidth requirements in your deployment to determine whether bandwidth between the locations can be increased.

However, note that increasing the bandwidth between these two locations means that you may need to reduce the bandwidth between other locations. Refer to the System Guide, SRNDs, and related Unified CM documentation for more details. Be aware that reducing the bandwidth or removing the higher bandwidth codecs from configuration may result in poor voice quality during call. Consider increasing the total amount of network bandwidth.

ApplicationConnectionDropped

Application has dropped the connection to CTIManager.

TCP or TLS connection between CTIManager and Application is disconnected.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Recommended Action

Possible causes include Application server power outage, network power outage, network configuration error, network delay, packet drops or packet corruption. It is also possible to get this error if the Unified CM node or application server is experiencing high CPU usage. Verify the application is up and running, verify network connectivity between the application server and Unified CM, and verify the CPU utilization is in the safe range for application server and Unified CM (this can be monitored using RTMT via CPU Pegging Alert).

ApplicationConnectionError

CTIManager is unable to allow connections from Applications.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

CTI Connection type(String)

Recommended Action

CTIManager has encountered problems initializing TCP connections. Restart the CTIManager service to resolve this problem.

authAdminLock

User is locked out by administrator.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Warning (4)

Parameters

lock(String)

Recommended Action

Administrator can unlock this user.

AuthenticationFailed

Login Authentication failed.

Facility/Sub-Facility

CCM_TOMCAT_APPS-LOGIN

Cisco Unified Serviceability Alarm Definition Catalog

System/Login

Severity

Warning

Parameters

Login IP Address/Hostname [String] Login Date/Time [String] Login UserID [String] Login Interface [String]

Recommended Action

If this event happens repeatedly, investigate the source of the failed login attempts.

authFail

Failed to authenticate this user.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.
8.0(1)	Changed severity level from Notice to Warning.

Cisco Unified CommunicationsRelease	Action
8.5(1)	Updated parameters.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Warning (4)

Parameters

UserID(String)

Message(String)

Recommended Action

Determine correct credentials and retry.

authHackLock

User attempted too many incorrect authentications. The maximum number of attempts gets set by the administrator.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.
8.0(1)	Added more descriptive text and corrected the parameter.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Warning (4)

Parameters

UserID(String)

Recommended Action

Wait for administrator specified time to retry, or have administrator unlock the credential.

authInactiveLock

The user has been inactive for a specified time and the credential is locked.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.
8.0(1)	Changed parameter text.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Warning (4)

Parameters

UserID(String)

Recommended Action

Reset credential.

authLdapInactive

Authentication failed because the user exists in the database and the system specifies LDAP authentication. A directory sync got performed in the immediate past (1 day).

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.
8.0(1)	Revised the description and added text to Recommended Action.
8.5(1)	Parameter updated.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Warning (4)

Parameters

UserID(String)

Recommended Action

This user has yet to be removed from the database or the alarm will clear itself within 24 hours.

BDIStopped

BDI Application stopped. Application was unloaded from Tomcat.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Warning (4)

Recommended Action

Check if Tomcat service is up.

CallAttemptBlockedByPolicy

A call was attempted but blocked or rejected by the policy decision point (PDP).

A call was rejected or blocked because it violated the enterprise policy as defined in a policy decision point (PDP) that was configured in Cisco Unified Communications Manager (Unified CM). The policy server returns a call reject decision stating that a policy violation was the reason for rejecting the call. Calls may be rejected because an unauthorized user attempted to dial a DN or pattern that is not allowed for him or her or because a call forward directive was invoked and the destination specified in the call forward operation violated the policy. Depending on email configuration in Real-Time Monitoring Tool (RTMT), the system may have generated an email alert when the call was rejected.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Alert Manager

Parameter(s)

Policy Decision Point(String)

Reject Reason(String)

Called Party Number(String)

Calling Party Number(String)

Calling User Id(String)

Recommended Action

Evaluate the information provided in this alarm (caller's user ID, to and from DNs, and so on) to determine if the call attempt was an innocent mistake to dial a number that the user didn't realize was not routable for him or her, or to discover whether the user is intentionally trying to circumvent the policy restrictions. If the rejected call was caused by an innocent mistake, educate the affected user about the numbers that he or she is allowed to dial. Your organization may have a policy or guidelines to follow when investigating call rejects. In addition to or instead of the steps recommended here, please refer to your company's guidelines.

CCDLearnedPatternLimitReached

CCD has reached the maximum number of learned patterns allowed.

The CCD requesting service has limited the number of learned patterns to a number defined in the service parameter, CCD Maximum Numbers of Learned Patterns. This alarm indicates that the CCD requesting service has met the maximum number of learned patterns allowed.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

CCD Maximum Numbers of Learned Patterns (UInt)

System Limit of CCD Learned Patterns (UInt)

Recommended Action

This alarm displays the value that is configured in the Cisco CallManager service parameter, CCD Maximum Numbers of Learned Patterns, as well as the maximum number of learned patterns that are allowed by the system (an internally-controlled maximum).

Consider whether the specified maximum number of learned patterns is correct for your deployment. If it is too low, compare it with the number shown in the SystemLimitCCDLearnedPatterns in this alarm. If the Max number is below the System Limit, you can go to the Service Parameters Configuration window and increase the CCD Maximum Numbers of Learned Patterns service parameter. If the Max and System Limit numbers match, the system is already configured to run at capacity of learned patterns; no action is required.

CDRHWMExceeded

The CDR files disk usage has exceeded the High Water Mark. CDRM deleted some successfully delivered CDR files that are still within the preservation duration, in order to bring the disk usage down to below HWM. E-mail alert will be sent to the admin.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Changed Data Collector Routing List element to Alert Manager.

Facility/Sub-Facility

CDRREP

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CDR Rep

Severity

Warning (4)

Routing List

Event Log

Sys Log

Alert Manager

Parameters

DiskUsageInMB [String]

Recommended Action

The preservation duration may be too long. Reduce it at **serviceability** > **tools** > **CDRM Configuration**.

Or raise maximum allocated disk space and/or HWM for CDR files.

CertValidLessThanMonth

Alarm indicates that the certificate will expire in 30 days or less.

Cisco Unified Serviceability Alarm Definition Catalog

System/CertMonitorAlarmCatalog

Severity

Warning(4)

Routing List

Event Log

Sys Log

Parameters

Message(String)

Recommended Action

Regenerate the certificate that is about to expire by accessing the Cisco Unified Operating System and go to Certificate Management. If the certificate is issued by a CA, generate a CSR, submit the CSR to CA, obtain a fresh certificate from CA, and upload it to Cisco Unified CM.

ConferenceNoMoreResourcesAvailable

Conference resource allocation failed for one or more of the following reasons: the required number of conference resources were not available; for an IOS-based conference bridge, the number of participants to be added to the conference bridge exceeded the maximum number of participants allowed per conference; no lower precedence conference was available for preemption although MLPP preemption was enabled; a lower-precedence conference bridge was not preempted.

Cisco Unified CommunicationsRelease	Action
8.0(1)	Changed severity level from Error to Warning.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Parameter(s)

Media Resource List Name(String)

Recommended Action

For IOS-based conference bridges, make sure that the maximum number of participants configured in a conference bridge does not exceed the number of participants allowed per conference; please check the IOS-based conference bridge user manual for limitations on the number of participants. Also, be sure to educate end users about the maximum number of participants allowed. For IOS-based and non-IOS-based, consider installing additional conference resources.

CtiDeviceOpenFailure

Application is unable to open the device.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiDeviceOpenFailure.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameter(s)

Device Name(String)

ReasonCode(Enum)

Recommended Action

Check the reason code and take appropriate action to resolve the issue.

Related Topics

Reason Code Enum Definitions for CtiDeviceOpenFailure, on page 238

Reason Code Enum Definitions for CtiDeviceOpenFailure

Value	Definition
0x8CCC0013 (2362179603)	Device is already opened by another application; identify the application that is controlling this device. You can determine this information from RTMT (**CallManager** > **CTI Manager and CallManager** > **CTI Search**)
0x8CCC00DA (2362179802)	Unable to communicate with database; verify the CPU utilization is in the safe range for (this can be monitored using RTMT via CPU Pegging Alert)
0x8CCC009A (2362179738)	Device is unregistering; wait for the device to register. Due to user initiated reset or restart of the device from Unified CM. Device should automatically register wait for few moments for the device to register
0x8CCC0018 (2362179608)	Device is not in the user control list; verify whether the device is configured for control by this application. For the application to control the device it should be included in the user control list. To check whether the device is in the user control list, if the application uses an End User, check the Device Association section under the End User Configuration in Cisco Unified CM Administration (**User Management** > **End User**). If the application uses an Application User, check under Device Information section for that Application User in Cisco Unified CM Administration (**User Management** > **Application User**)
0x8CCC00F3 (2362179827)	IPAddress mode (IPv4 or IPv6 or both) specified by the application does not match with IP Addressing mode that is configured in Unified CM Administration; check the IP addressing mode of the device in Cisco Unified CM Administration (**Device** > **Device Settings** > **Common Device Configuration**)

CtiLineOpenFailure

Application is unable to open the line.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiLineOpenFailure.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameter(s)

Device Name(String)

Directory Number(String)

Partition(String)

Reason(Enum)

Recommended Action

Review the reason code and take appropriate action to resolve the issue.

Related Topics

Reason Code Enum Definitions for CtiLineOpenFailure, on page 239

Reason Code Enum Definitions for CtiLineOpenFailure

Value	Definition
0	Unknown

Value	Definition
0x8CCC0018 (2362179608)	Device is not in the user control list; verify whether the device is configured for control by this application. For the application to control the device it should be included in the user control list. To check whether the device is in the user control list, if the application uses an End User, check the Device Association section under the End User Configuration in Cisco Unified CM Administration (**User Management** > **End User**). If the application uses an Application User, check under Device Information section for that Application User in Cisco Unified CM Administration (**User Management** > **Application User**)
0x8CCC0005 (2362179589)	Line is not found in the device; possible cause could be that the line that previously existed on this device is not available. This could be due to a extension mobility login or logout
0x8CCC00D3 (2362179795)	Administrator has restricted the Line to be controllable by application. If the intent of the Administrator is to allow control of this line, enable the check box labelled Allow control of Device from CTI, in Unified CM Administration under **Call Routing** > **Directory Number** and choose the line that should be controlled by this application

CtiIncompatibleProtocolVersion

Incompatible protocol version.

The JTAPI/TAPI application version is not compatible with this version of CTIManager, so the received message has been rejected. The IP address is shown in either IPv4 or IPv6 format depending on the IP addressing mode of the Application.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiIncompatibleProtocolVersion.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Unified CM Version(String)

IPAddress(String)

IPv6Address(String)

Recommended Action

Verify that the correct version of the application is being used. If you are not sure of the correct version, contact the application vendor and upgrade the JTAPI/TSP to the version provided by Cisco Unified Communications Manager. JTAPI/TSP plugins are available in Cisco Unified CM Administration (**Application** > **Plugins**).

CtiMaxConnectionReached

Maximum number of CTI connections has been reached, no new connection will be accepted unless an existing connection is closed.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiMaxConnectionReached.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Recommended Action

Check the CTI Manager service parameter Maximum CTI Connections for the maximum number of connections. Carefully, consider increasing the service parameter value or disconnecting CTI applications that are unnecessary. Refer to Unified CM Solution Reference Network Design document in www.cisco.com based on the version you are using for maximum number of applications and devices supported by CTI.

CtiProviderCloseHeartbeatTimeout

CTI heartbeat timeout occurred causing CTIManager to close the application connection.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiProviderCloseHeartbeatTimeout.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Recommended Action

Heartbeat timeout could occur due to high CPU usage or network connectivity problems. Check for and fix any network issues or high CPU usage on the application server. If the application server is running the Microsoft Windows OS use Task Manager or Perfmon to determine the CPU usage. For applications in Linux use the top command to review CPU usage.

CtiQbeFailureResponse

The requested operation from the application could not be performed because of a normal or abnormal condition.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiQbeFailureResponse.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Error message(String)

Recommended Action

Verify whether the affected application is experiencing a problem. Contact the support organization for the affected application if the problem persists and provide sequence number and error message for further investigation.

DaTimeOut

The digit analysis component in Cisco Unified Communications Manager has timed out. This can occur because Cisco Unified Communications Manager is busy and the resulting delay in processing request and response messages caused the digit analysis component to time out.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Recommended Action

In the Service Parameter Configuration window in Cisco Unified CM Administration, check the Cisco CallManager service parameter, Digit Analysis Timer, to confirm that the default value is in use. Use RTMT to monitor the system resources and correct any system issues that might be contributing to high CPU utilization on Cisco Unified CM.

DeviceImageDownloadFailure

Cisco IP Phone failed to download its image.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	Enum Definitions for FailureReason.
7.1	Added DeviceImageDownloadFailure to the Phone Catalog.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/Phone

Severity

Warning (4)

Parameters

DeviceName(String)

IPAddress(String)

Active(String)

Inactive(String)

FailedLoadId(String)

Method(Enum)

FailureReason(Enum)

Server(String)

Recommended Action

Verify that the IP address or hostname of the image download server (either the Load server or the TFTP server) is correct. If you're using a hostname, verify that the Domain Name Server (DNS) is accessible from the phone and can resolve the hostname. Verify that the TFTP service is activated and running on the Load server or TFTP server (the server you are using to serve firmware load files). Verify that the Load server or TFTP server is accessible from the phone. Also, refer to the reason code descriptions for recommended actions.

Related Topics

Method Enum Definitions for DeviceImageDownloadFailure, on page 245
FailureReason Enum Definitions for DeviceImageDownloadFailure, on page 245

Method Enum Definitions for DeviceImageDownloadFailure

Code	Definition
1	TFTP
2	HTTP
3	PPID

FailureReason Enum Definitions for DeviceImageDownloadFailure

Code	Definition
1	A TFTP server error occurred - examine the TFTP log to determine whether other errors occurred at the same time the device was attempting to download its firmware and correct any TFTP errors that may have occurred. Also, investigate the load on the TFTP server to ensure that device download requests are being processed; check network connectivity to the TFTP server.
2	Specified firmware load ID is not found on the TFTP server. Check that file name is correct, or load (image) file exist on TFTP server.
3	An internal phone error occurred during the download attempt; reset the phone to correct the issue.
4	The Load server or TFTP server could not process the phone's firmware load request. It is possible that congestion is causing a delay in TFTP response. To allow the phone to attempt the download again, wait a few minutes then reset the phone. The phone will attempt to download its firmware load again. If resetting the phone does not solve the issue, restart the Load server or TFTP server (whichever server provides firmware loads).
5	An encryption error occurred on the phone while trying to load the new firmware load (image); reset the phone to correct the issue.
6	The downloaded firmware load (image) is not encrypted. Verify that correct load (image) name is provided to the phone and that the server that provides firmware loads has that encrypted load (image) file.

Code	Definition
7	The downloaded firmware load (image) cannot be decrypted using the decryption key on the phone (resulting in an encryption key mismatch). If you have provided the image encryption key, try re-encrypting the image with the key that matches the key already on the phone, then attempt the download again. Otherwise, collect the phone logs from the time of this alarm (review the steps in the Administration Guide for the appropriate phone model to learn how to access the phone logs) and contact the Cisco Technical Assistance Center (TAC).
8	There is a problem with the encryption of the downloaded firmware load (image). Collect pertinent details such as the device's MAC address, device type, the firmware load ID, and phone logs from the time of this alarm (review the steps in the Administration Guide for the appropriate phone model to learn how to access the phone logs), and contact the Cisco Technical Assistance Center (TAC).
9	The phone did not receive a load server name or IP address and as a result, does not have the server information needed to download a firmware load. Check the Device Configuration page in Cisco Unified CM Administration to ensure that the IP address of the Load server or TFTP server is accurately configured. If the information is inaccurate or not present, supply the correct information and restart the phone. If the information is accurate, restart the phone. If this alarm recurs, contact the Cisco Technical Assistance Center (TAC).
10	The phone attempted an action that is not allowed by the Load server or TFTP server; reset the phone to attempt to clear the condition.
13	The device has exceeded the internally-configured time allowed for a response from the Load server or TFTP server when requesting the firmware load file. It is possible that congestion is causing a delay in TFTP response. To allow the phone to attempt the download again, wait a few minutes then reset the phone. The phone will attempt to download the file again. If resetting the phone does not solve the issue, restart the Load server or TFTP server (whichever server provides the firmware load files).
14	The data that the phone received from the Load server or TFTP server was not intact; not enough information was received. Restart the phone to begin the download process again.
15	The data that the phone received from the Load server or TFTP server was not intact; too much information was received. Restart the phone to begin the download process again.
16	The phone cannot connect to the network; check for network connectivity to the image firmware load server or the TFTP server and correct any broken connection. Restart the phone to attempt connection again unless the restart occurs automatically.
17	The DNS server name that the phone is attempting to connect to could not be resolved. Examine the DNS server name(s) in the phone settings to verify that the information is accurate and if not, update the name on the phone. Restart the phone unless the restart occurs automatically.
18	No DNS server - Configure a DNS server IP address on the phone settings. Restart the phone unless the restart occurs automatically.

Code	Definition
19	Connection to the Load server or TFTP server has timed out - The phone attempted to connect to the Load server or TFTP server but could not connect successfully. If you are using the TFTP server to serve firmware loads, check the TFTP server IP address as configured in the settings on the phone; make sure the IP address is accurate. If it is not, correct the IP address and press Apply; the phone should restart automatically. If you are using a Load server to serve firmware loads, check the IP address or hostname on the Phone Configuration page in Cisco Unified CM Administration for the phone identified in this alarm, to ensure that the information is accurate. If it is not, update the IP address or hostname and restart the phone. Also, verify that network connectivity exists between the phone and the Load server or TFTP server. Restart the phone to attempt connection again unless the restart occurs automatically.
20	Download was cancelled - A previous download request was superseded by a new download request. The original download was cancelled so that the new download could continue. No action is required.

DevicePartiallyRegistered

Device partially registered. A device is partially registered with Cisco CallManager. Some, but not all, of the lines configured on the device have successfully registered.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Following information is updated: • Enum Definitions for performance monitor object type • Enum Definitions for DeviceType

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning (4)

Parameters

Device name. [String] Device MAC address [Optional]. [String] Device IP address. [String] Protocol. [String] Device description [Optional]. [String] User ID [Optional]. [String] Load ID. [Optional] [String] Associated directory numbers. [String] Performance monitor object type [Enum]Device type. [Optional] [Enum]

Recommended Action

In the Cisco Unified Reporting tool, run the Unified CM Multi-Line Devices report and check the number of lines that are supposed to be configured on the device identified in this alarm. If the device has registered an inconsistent number of lines compared the Multi-Lines report for this device, restart the device so that it can reregister all lines. If this alarm persists, verify that the appropriate number of lines has been configured on the device, and that the appropriate directory numbers have been configured. If the device is a third-party SIP phone, verify that the directory numbers configured on the phone match the directory numbers configured on the device in Unified CM Administration.

Related Topics

Performance Monitor Object Type Enum Definitions for DevicePartiallyRegistered, on page 248
DeviceType Enum Definitions for DevicePartiallyRegistered, on page 249

Performance Monitor Object Type Enum Definitions for DevicePartiallyRegistered

Code	Reason
1	Cisco CallManager
2	Cisco Phones
3	Cisco Lines
4	Cisco H323
5	Cisco MGCP Gateway
6	Cisco MOH Device
7	Cisco Analog Access
8	Cisco MGCP FXS Device
9	Cisco MGCP FXO Device
10	Cisco MGCP T1CAS Device
11	Cisco MGCP PRI Device

DeviceType Enum Definitions for DevicePartiallyRegistered

Code	Reason
1	CISCO_30SP+
2	CISCO_12SP+
3	CISCO_12SP
4	CISCO_12S
5	CISCO_30VIP
6	CISCO_7910
7	CISCO_7960
8	CISCO_7940
9	CISCO_7935
10	CISCO_VGC_PHONE
11	CISCO_VGC_VIRTUAL_PHONE
12	CISCO_ATA_186
20	SCCP_PHONE
30	ANALOG_ACCESS
40	DIGITAL_ACCESS
42	DIGITAL_ACCESS+
43	DIGITAL_ACCESS_WS-X6608
47	ANALOG_ACCESS_WS-X6624
48	VGC_GATEWAY
50	CONFERENCE_BRIDGE
51	CONFERENCE_BRIDGE_HARDWARE
52	CONFERENCE_BRIDGE_HARDWARE_HDV2
53	CONFERENCE_BRIDGE_HARDWARE_WS-SVC-CMM

Code	Reason
61	H323_PHONE
62	H323_GATEWAY
70	MUSIC_ON_HOLD
71	DEVICE_PILOT
72	CTI_PORT
73	CTI_ROUTE_POINT
80	VOICE_MAIL_PORT
83	SOFTWARE_MEDIA_TERMINATION_POINT_HDV2
84	CISCO_MEDIA_SERVER
85	CISCO_VIDEO_CONFERENCE_BRIDGE
90	ROUTE_LIST
100	LOAD_SIMULATOR
110	MEDIA_TERMINATION_POINT
111	MEDIA_TERMINATION_POINT_HARDWARE
112	MEDIA_TERMINATION_POINT_HDV2
113	MEDIA_TERMINATION_POINT_WS-SVC-CMM
115	CISCO_7941
119	CISCO_7971
120	MGCP_STATION
121	MGCP_TRUNK
122	GATEKEEPER
124	7914_14_BUTTON_LINE_EXPANSION_MODULE
125	TRUNK
126	TONE_ANNOUNCEMENT_PLAYER

Code	Reason
131	SIP_TRUNK
132	SIP_GATEWAY
133	WSM_TRUNK
134	REMOTE_DESTINATION_PROFILE
227	7915_12_BUTTON_LINE_EXPANSION_MODULE
228	7915_24_BUTTON_LINE_EXPANSION_MODULE
229	7916_12_BUTTON_LINE_EXPANSION_MODULE
230	7916_24_BUTTON_LINE_EXPANSION_MODULE
232	CKEM_36_BUTTON_LINE_EXPANSION_MODULE
254	UNKNOWN_MGCP_GATEWAY
255	UNKNOWN
302	CISCO_7989
307	CISCO_7911
308	CISCO_7941G_GE
309	CISCO_7961G_GE
335	MOTOROLA_CN622
336	BASIC_3RD_PARTY_SIP_DEVICE
348	CISCO_7931
358	CISCO_UNIFIED_COMMUNICATOR
365	CISCO_7921
369	CISCO_7906
374	ADVANCED_3RD_PARTY_SIP_DEVICE
375	CISCO_TELEPRESENCE
404	CISCO_7962

Code	Reason
412	CISCO_3951
431	CISCO_7937
434	CISCO_7942
435	CISCO_7945
436	CISCO_7965
437	CISCO_7975
446	CISCO_3911
468	CISCO_UNIFIED_MOBILE_COMMUNICATOR
478	CISCO_TELEPRESENCE_1000
479	CISCO_TELEPRESENCE_3000
480	CISCO_TELEPRESENCE_3200
481	CISCO_TELEPRESENCE_500
484	CISCO_7925
493	CISCO_9971
495	CISCO_6921
496	CISCO_6941
497	CISCO_6961
20000	CISCO_7905
30002	CISCO_7920
30006	CISCO_7970
30007	CISCO_7912
30008	CISCO_7902
30016	CISCO_IP_COMMUNICATOR
30018	CISCO_7961

Code	Reason
30019	CISCO_7936
30027	ANALOG_PHONE
30028	ISDN_BRI_PHONE
30032	SCCP_GATEWAY_VIRTUAL_PHONE
30035	IP_STE

DeviceTransientConnection

A connection was established and immediately dropped before completing registration. Incomplete registration may indicate that a device is rehoming in the middle of registration. The alarm could also indicate a device misconfiguration, database error, or an illegal/unknown device trying to attempt a connection. Network connectivity problems can affect device registration, or the restoration of a primary Unified CM may interrupt registration.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Error to Warning. • Following information is updated: ◦ Enum Definitions for DeviceType ◦ Enum Definitions ◦ Enum Definitions for IPAddrAttributes ◦ Enum Definitions for IPV6AddrAttributes
7.1	IPv6 parameters added: IPV6Address[Optional][String], IPAddrAttributes[Optional][Enum], and IPV6AddrAttributes[Optional][Enum].

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Parameters

Device IP address [Optional].[String]

Device name [Optional].[String]

Device MAC address [Optional].[String]

Protocol.[String]

Device type. [Optional][Enum]

Reason Code [Optional].[Enum]

Connecting Port [UInt]

Registering SIP User. [Optional].[String]

IPV6Address [Optional].[String]

IPAddressAttributes [Optional].[Enum]

IPV6AddressAttributes [Optional].[Enum]

Recommended Action

In the Cisco Unified Reporting tool, check the Active Services section of the Unified CM Cluster Overview report to confirm that any failover/fallback scenarios have completed. Confirm that auto-registration is enabled if the phone attempting to connect is set to auto-register, or locate the phone that is attempting to auto-register if auto-registration has been intentionally disabled. Check the device indicated in this alarm and confirm that the device registration details in Cisco Unified CM Administration are accurate. Also, refer to the reason code definitions for recommended actions. No action is required if this event was issued as a result of a normal device rehome.

Related Topics

DeviceType Enum Definitions for DeviceTransientConnection, on page 254
Enum Definitions for DeviceTransientConnection, on page 256
IPAddrAttributes Enum Definitions for DeviceTransientConnection, on page 259
IPV6AddrAttributes Enum Definitions for DeviceTransientConnection, on page 259

DeviceType Enum Definitions for DeviceTransientConnection

Code	Reason
10	CISCO_VGC_PHONE
11	CISCO_VGC_VIRTUAL_PHONE
30	ANALOG_ACCESS
40	DIGITAL_ACCESS
42	DIGITAL_ACCESS+

Code	Reason
43	DIGITAL_ACCESS_WS-X6608
47	ANALOG_ACCESS_WS-X6624
48	VGC_GATEWAY
50	CONFERENCE_BRIDGE
51	CONFERENCE_BRIDGE_HARDWARE
52	CONFERENCE_BRIDGE_HARDWARE_HDV2
53	CONFERENCE_BRIDGE_HARDWARE_WS-SVC-CMM
62	H323_GATEWAY
70	MUSIC_ON_HOLD
71	DEVICE_PILOT
73	CTI_ROUTE_POINT
80	VOICE_MAIL_PORT
83	SOFTWARE_MEDIA_TERMINATION_POINT_HDV2
84	CISCO_MEDIA_SERVER
85	CISCO_VIDEO_CONFERENCE_BRIDGE
90	ROUTE_LIST
100	LOAD_SIMULATOR
110	MEDIA_TERMINATION_POINT
111	MEDIA_TERMINATION_POINT_HARDWARE
112	MEDIA_TERMINATION_POINT_HDV2
113	MEDIA_TERMINATION_POINT_WS-SVC-CMM
120	MGCP_STATION
121	MGCP_TRUNK
122	GATEKEEPER

Code	Reason
124	7914_14_BUTTON_LINE_EXPANSION_MODULE
125	TRUNK
126	TONE_ANNOUNCEMENT_PLAYER
131	SIP_TRUNK
132	SIP_GATEWAY
133	WSM_TRUNK
134	REMOTE_DESTINATION_PROFILE
227	7915_12_BUTTON_LINE_EXPANSION_MODULE
228	7915_24_BUTTON_LINE_EXPANSION_MODULE
229	7916_12_BUTTON_LINE_EXPANSION_MODULE
230	7916_24_BUTTON_LINE_EXPANSION_MODULE
232	CKEM_36_BUTTON_LINE_EXPANSION_MODULE
254	UNKNOWN_MGCP_GATEWAY
255	UNKNOWN
30027	ANALOG_PHONE
30028	ISDN_BRI_PHONE
30032	SCCP_GATEWAY_VIRTUAL_PHONE

Enum Definitions for DeviceTransientConnection

Code	Reason
1	Unknown—(SCCP only) The device failed to register for an unknown reason. If this persists, collect SDL/SDI traces with “Enable SCCP Keep Alive Trace” enabled and contact TAC.
2	NoEntryInDatabase—(MGCP only) The device is not configured in the Unified CM Administration database and auto-registration is either not supported for the device type or is not enabled. To correct this problem, configure this device in Unified CM Administration.

Code	Reason
3	DatabaseConfigurationError—The device is not configured in the Unified CM Administration database and auto-registration is either not supported for the device type or is not enabled. To correct this problem, configure this device in Unified CM Administration.
4	DeviceNameUnresolveable—For SIP third-party devices this means that Unified CM could not determine the name of the device from the Authorization header in the REGISTER message. The device did not provide an Authorization header after Unified CM challenged with a 401 Unauthorized message. Verify that the device is configured with digest credentials and is able to respond to 401challenges with an Authorization header. If this is a Cisco IP phone, the configuration may be out-of-sync. First, go to the Cisco Unified Reporting web page, generate a Unified CM Database Status report, and verify "all servers have a good replication status". If DB replications looks good, reset the phone. If that still doesn't fix the problem, restart the TFTP and the Cisco CallManager services. For all other devices, this reason code means that DNS lookup failed. Verify the DNS server configured via the OS Administration CLI is correct and that the DNS name used by the device is configured in the DNS server.
6	ConnectivityError—The network connection between the device and Cisco Unified CM dropped before the device was fully registered. Possible causes include device power outage, network power outage, network configuration error, network delay, packet drops and packet corruption. It is also possible to get this error if the Cisco Unified CM node is experiencing high CPU usage. Verify the device is powered up and operating, verify network connectivity between the device and Cisco Unified CM, and verify the CPU utilization is in the safe range (this can be monitored using RTMT via CPU Pegging Alert).
7	InitializationError—An internal error occurred within Cisco Unified CM while processing the device registration. It is recommended to restart the Cisco CallManager service. If this occurs repeatedly, collect SDL/SDI detailed traces with "Enable SIP Keep Alive (REGISTER Refresh) Trace" and "Enable SCCP Keep Alive Trace" under Cisco CallManager services turned on and contact TAC.
10	AuthenticationError—The device failed either TLS or SIP digest security authentication. If the device is a SIP phone and is enabled for digest authentication (on the **System** > **Security Profile** > **Phone Security Profile**, check if "Enable Digest Authentication" checkbox is checked), verify the "Digest Credentials" in the End User config page are configured. Also, check the phone config page to see if the phone is associated with the specified end user in the Digest User drop box. If the device is a third-party SIP device, verify the digest credentials configured on the phone match the "Digest Credentials" configured in the End User page.

Code	Reason
11	InvalidX509NameInCertificate—Configured “X.509 Subject Name” doesn't match what's in the certificate from the device. Check the Security profile of the indicated device and verify the “Device Security Mode” is either “Authenticated” or “Encrypted”. Verify the “X.509 Subject Name” field has the right content. It should match the Subject Name in the certificate from the peer.
12	InvalidTLSCipher—Unsupported cipher algorithm used by the device; Cisco Unified CM only supports AES_128_SHA cipher algorithm. Recommended action is for the device to regenerate its certificate with the AES_128_SHA cipher algorithm.
14	MalformedRegisterMsg—(SIP only) A SIP REGISTER message could not be processed because of an illegal format. Possible causes include a missing Call-ID header, a missing AoR in the To header, and an expires value too small. Verify the REGISTER message does not suffer from any of these ills.
15	ProtocolMismatch—The protocol of the device (SIP or SCCP) does not match the configured protocol in Cisco Unified CM. Recommended actions: **1** Verify the device is configured with the desired protocol. **2** Verify the firmware load ID on the Device Defaults page is correct and actually exists on the TFTP server. **3** If there is a firmware load ID configured on the device page, verify it is correct and exists on the TFTP server (On Cisco Unified OS Administration page, **Software Upgrades** > **TFTP File Management**, look for the file name as specified by load ID). **4** Restart the TFTP and Cisco CallManager services. Use the Cisco Unified OS Administration TFTP File Management page to verify the configured firmware loads exist.
16	DeviceNotActive—The device has not been activated
17	AuthenticatedDeviceAlreadyExists—A device with the same name is already registered. If this occurs repeatedly, collect SDL/SDI detailed traces with “Enable SIP Keep Alive (REGISTER Refresh) Trace” and “Enable SCCP Keep Alive Trace” under Cisco CallManager services turned on and contact TAC. There may be an attempt by unauthorized devices to register.
18	ObsoleteProtocolVersion—(SCCP only) A SCCP device registered with an obsolete protocol version. Power cycle the phone. Verify that the TFTP service is activated. Verify that the TFTP server is reachable from the device. If there is a firmware load ID configured on the Phone Config page, verify that the firmware load ID exists on the TFTP server (On Cisco Unified OS Administration page, **Software Upgrades** > **TFTP File Management**, look for the file name as specified by load ID).

IPAddrAttributes Enum Definitions for DeviceTransientConnection

Code	Reason
0	Unknown—The device has not indicated what this IPv4 address is used for.
1	Administrative only—The device has indicated that this IPv4 address is used for administrative communication (web interface) only.
2	Signal only—The device has indicated that this IPv4 address is used for control signaling only.
3	Administrative and signal—The device has indicated that this IPv4 address is used for administrative communication (web interface) and control signaling.

IPV6AddrAttributes Enum Definitions for DeviceTransientConnection

Code	Reason
0	Unknown—The device has not indicated what this IPv6 address is used for.
1	Administrative only—The device has indicated that this IPv6 address is used for administrative communication (web interface) only.
2	Signal only—The device has indicated that this IPv6 address is used for control signaling only.
3	Administrative and signal—The device has indicated that this IPv6 address is used for administrative communication (web interface) and control signaling.

DeviceUnregistered

A device that has previously registered with Cisco CallManager has unregistered. In cases of normal unregistration with reason code “CallManagerReset”, “CallManagerRestart”, or “DeviceInitiatedReset”, the severity of this alarm is lowered to INFORMATIONAL. A device can unregister for many reasons, both intentional, such as manually resetting the device after a configuration change, or unintentional, such as loss of network connectivity. Other causes for this alarm could include a phone being registered to a secondary node and then the primary node come back online, causing the phone to rehome to the primary Unified CM node or lack of a KeepAlive being returned from the Unified CM node to which this device was registered. Unregistration also occurs if Unified CM receives a duplicate registration request for this same device.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Error to Warning. • Following information is updated: ◦ Enum Definitions for DeviceType ◦ Enum Definition ◦ Enum Definitions for IPAddrAttributes ◦ Enum Definitions for IPV6AddrAttributes
7.1	Parameters added: IPV6Address,IPAddrAttributes, and IPV6AddrAttributes.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Parameters

Device name. [String]

Device MAC address [Optional]. [String]

Device IP address [Optional]. [String]

Protocol. [String]

Device type. [Optional] [Enum]

Device description [Optional]. [String]

Reason Code [Optional]. [Enum]

IPV6Address [Optional]. [String]

IPAddressAttributes [Optional]. [Enum]

IPV6AddressAttributes [Optional]. [Enum]

See the following:

Recommended Action

Actions to take vary depending on the reason specified for the device unregistration. If the reason is ConfigurationMismatch, go to the Device Configuration page in Cisco Unified CM Administration, make a change to the Description field for this device, click Save, then reset the device. In the case of a network connectivity or loss of KeepAlives problem, use network diagnostic tools and the Cisco Unified CM Reporting tool to fix any reported network or Unified CM system errors. In the case of a device rehoming to the primary Unified CM node, watch for a successful registration of the device on the primary node. In the case of a duplicate registration request, it may be a non-malicious occurrence due to timing of a device registering and unregistering; if duplicate registration requests continue or if the same device has different IP addresses, confirm the IP address on the physical device itself by checking the settings on the device (settings button). If unregistration of this device was expected, no action is required. Also, refer to the reason code descriptions for recommended actions.

Related Topics

DeviceType Enum Definitions for DeviceUnregistered, on page 261
Enum Definitions for DeviceUnregistered, on page 263
IPAddrAttributes Enum Definitions for DeviceUnregistered, on page 265
IPV6AddrAttributes Enum Definitions for DeviceUnregistered, on page 265

DeviceType Enum Definitions for DeviceUnregistered

Code	Device Type
10	CISCO_VGC_PHONE
11	CISCO_VGC_VIRTUAL_PHONE
30	ANALOG_ACCESS
40	DIGITAL_ACCESS
42	DIGITAL_ACCESS+
43	DIGITAL_ACCESS_WS-X6608
47	ANALOG_ACCESS_WS-X6624
48	VGC_GATEWAY
50	CONFERENCE_BRIDGE
51	CONFERENCE_BRIDGE_HARDWARE
52	CONFERENCE_BRIDGE_HARDWARE_HDV2
53	CONFERENCE_BRIDGE_HARDWARE_WS-SVC-CMM
62	H323_GATEWAY

Code	Device Type
70	MUSIC_ON_HOLD
71	DEVICE_PILOT
73	CTI_ROUTE_POINT
80	VOICE_MAIL_PORT
83	SOFTWARE_MEDIA_TERMINATION_POINT_HDV2
84	CISCO_MEDIA_SERVER
85	CISCO_VIDEO_CONFERENCE_BRIDGE
90	ROUTE_LIST
100	LOAD_SIMULATOR
110	MEDIA_TERMINATION_POINT
111	MEDIA_TERMINATION_POINT_HARDWARE
112	MEDIA_TERMINATION_POINT_HDV2
113	MEDIA_TERMINATION_POINT_WS-SVC-CMM
120	MGCP_STATION
121	MGCP_TRUNK
122	GATEKEEPER
124	7914_14_BUTTON_LINE_EXPANSION_MODULE
125	TRUNK
126	TONE_ANNOUNCEMENT_PLAYER
131	SIP_TRUNK
132	SIP_GATEWAY
133	WSM_TRUNK
134	REMOTE_DESTINATION_PROFILE
227	7915_12_BUTTON_LINE_EXPANSION_MODULE

Code	Device Type
228	7915_24_BUTTON_LINE_EXPANSION_MODULE
229	7916_12_BUTTON_LINE_EXPANSION_MODULE
230	7916_24_BUTTON_LINE_EXPANSION_MODULE
232	CKEM_36_BUTTON_LINE_EXPANSION_MODULE
254	UNKNOWN_MGCP_GATEWAY
255	UNKNOWN
30027	ANALOG_PHONE
30028	ISDN_BRI_PHONE
30032	SCCP_GATEWAY_VIRTUAL_PHONE

Enum Definitions for DeviceUnregistered

Code	Reason
1	Unknown - The device has unregistered for an unknown reason. If the device does not reregister within 5 minutes, verify it is powered-up and verify network connectivity between the device and Cisco Unified CM.
6	ConnectivityError - Network communication between the device and Cisco Unified CM has been interrupted. Possible causes include device power outage, network power outage, network configuration error, network delay, packet drops and packet corruption. It is also possible to get this error if the Cisco Unified CM node is experiencing high CPU usage. Verify the device is powered up and operating, verify network connectivity between the device and Cisco Unified CM, and verify the CPU utilization is in the safe range (this can be monitored using RTMT via CPU Pegging Alert).
8	DeviceInitiatedReset - The device has initiated a reset, possibly due to a power cycle or internal error. No action required; the device will reregister automatically.
9	CallManagerReset - A device reset was initiated from Cisco Unified CM Administration, either due to an explicit command from an administrator, or due to internal errors encountered. No action necessary, the device will reregister automatically.
10	DeviceUnregistered - The device has explicitly unregistered. Possible causes include a change in the IP address or port of the device. No action is necessary, the device will reregister automatically.

Code	Reason
11	MalformedRegisterMsg - (SIP only) A SIP REGISTER message could not be processed because of an illegal format. Possible causes include a missing Call-ID header, a missing AoR in the To header, and an expires value too small. Verify the REGISTER message does not suffer from any of these ills.
12	SCCPDeviceThrottling - (SCCP only) The indicated SCCP device exceeded the maximum number of events allowed per-SCCP device. Events can be phone calls, KeepAlive messages, or excessive SCCP or non-SCCP messages. The maximum number of allowed events is controlled by the Cisco CallManager service parameter, Max Events Allowed. When an individual device exceeds the number configured in that service parameter, Unified CM closes the TCP connection to the device; automatic reregistration generally follows. This action is an attempt to stop malicious attacks on Unified CM or to ward off excessive CPU usage.
13	KeepAliveTimeout - A keepalive message was not received. Possible causes include device power outage, network power outage, network configuration error, network delay, packet drops and packet corruption. It is also possible to get this error if the Cisco Unified CM node is experiencing high CPU usage. Verify the device is powered up and operating, verify network connectivity between the device and Cisco Unified CM, and verify the CPU utilization is in the safe range (this can be monitored using RTMT via CPU Pegging Alert).
14	ConfigurationMismatch (SIP only) The configuration on the device does not match the configuration in Cisco Unified CM. This can be caused by database replication errors or other internal Cisco Unified CM communication errors. First go to the Cisco Unified Reporting web page, generate a Unified CM Database Status report, and verify "all servers have a good replication status". If this device continues to unregister with this reason code, go to the CCMAdmin Device web page for the device and click Save. This allows a change notify to be generated to the Unified CM and TFTP services and rebuild a new config file. If the problem still persists, restart the TFTP service and Cisco Unified CM service.
15	CallManagerRestart - A device restart was initiated from Cisco Unified CM, either due to an explicit command from an administrator, or due to a configuration change such as adding, deleting or changing a DN associated with the device. No action necessary, the device will reregister automatically.
16	DuplicateRegistration - Cisco Unified CM detected that the device attempted to register to 2 nodes at the same time. Cisco Unified CM initiated a restart to the phone to force it to rehome to a single node. No action necessary, the device will reregister automatically.
17	CallManagerApplyConfig - An ApplyConfig command was invoked from Unified CM Administration resulting in an unregistration. No action necessary, the device will reregister automatically.

Code	Reason
18	DeviceNoResponse - The device did not respond to a reset or restart notification, so it is being forcefully reset. If the device does not reregister within 5 minutes, confirm it is powered-up and confirm network connectivity between the device and Cisco Unified CM.

IPAddrAttributes Enum Definitions for DeviceUnregistered

Code	Reason
0	Unknown—The device has not indicated what this IPv4 address is used for.
1	Administrative only—The device has indicated that this IPv4 address is used for administrative communication (web interface) only.
2	Signal only—The device has indicated that this IPv4 address is used for control signaling only.
3	Administrative and signal—The device has indicated that this IPv4 address is used for administrative communication (web interface) and control signaling.

IPV6AddrAttributes Enum Definitions for DeviceUnregistered

Code	Reason
0	Unknown - The device has not indicated what this IPv6 address is used for
1	Administrative only - The device has indicated that this IPv6 address is used for administrative communication (web interface) only.
2	Signal only - The device has indicated that this IPv6 address is used for control signaling only.
3	Administrative and signal - The device has indicated that this IPv6 address is used for administrative communication (web interface) and control signaling.

DigitAnalysisTimeoutAwaitingResponse

Cisco Unified Communications Manager sent a routing request to the policy decision point but the request timed out without a response.

Cisco Unified Communications Manager (Unified CM) was unable to complete the routing request before timing out. This time out could occur due to low system resources, high CPU usage, or a high volume of call

activities on this Unified CM node. Unified CM applies the Call Treatment on Failure that is configured for the External Call Control Profile associated with this call.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Translation Pattern Triggering Point(String)

Policy Decision Point(String)

Recommended Action

- Check the External Call Control object in Real-Time Monitoring Tool (RTMT) to see whether the ExternalCallControlEnabledCallAttempted counter is spiking. If so, this indicates an unusually high number of calls at this time which could result in reduced system resources.
- Check the QueueSignalsPresent2-Normal for persistent long high signal queue. If the long signal queue exists, check whether the Code Yellow alarm has already issued and check the system CPU and memory usage for this Unified CM node.
- Follow the recommended actions for Code Yellow alarm if the Code Yellow alarm has fired.

For high CPU usage, use RTMT to determine which areas may be contributing to the high CPU usage. If this alarm persists, collect system performance data (such as the percentage of Memory, Page and VM usage, partition read and write bytes per second, the percentage of CPU usages of all the processes, and the processor IOWait percentage) and contact Cisco Technical Assistance Center (TAC).

DirSyncNoSchedulesFound

No schedules found in DB for directory synchronization. No automatic LDAP directory synchronization possible.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Warning (4)

Parameters

ScheduleTableName [String]

Recommended Action

Check the DirSync configuration

DirSyncScheduledTaskTimeoutOccurred

Timeout occurred for directory synchronization task.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Warning (4)

Parameters

SchedulerID [String] TaskID [String]

Recommended Action

Check the DirSync configuration.

DRFComponentDeRegistered

DRF successfully de-registered the requested component.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFComponentDeRegistered. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Warning (4)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Ensure that the component that was de-registered is not needed for further backup/restore operation.

DRFDeRegistrationFailure

DRF de-registration request for a component failed.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFDeRegistrationFailure. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Warning (4)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Check the DRF logs and contact support if needed.

DRFDeRegisteredServer

DRF automatically de-registered all the components for a server. This server might have got disconnected from CCM cluster.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFDeRegisteredServer. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Warning (4)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

None

DRFNoBackupTaken

A valid backup of the current system was not found after an Upgrade, Migration, or Fresh Install.

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

WARNING

Routing List

Event Log

Sys Log

Parameter(s)

Reason(String)

Recommended Action

It is recommended to perform a Backup using the Disaster Recovery System.

DRFSchedulerDisabled

DRF Scheduler is disabled because no configured features available for backup.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from CiscoDRFSchedulerDisabled. Routing List elements added.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Warning (4)

Routing List

Event Log

Sys Log

Parameters

Reason(String)

Recommended Action

Ensure at least one feature is configured for the scheduled backup to run.

EMCCFailedInRemoteCluster

There was an EMCC login failure at a remote Unified CM. EMCC login could fail due to the following reasons:

- User does not exist in any of the configured remote cluster.
- User is not enabled for EMCC.
- No free EMCC base device.
- EMCC access was prevented by remote cluster.
- Untrusted certificate received from the remote end while trying to establish a connection.

Reason Codes:

- 38—EMCC or PSTN is not activated in InterClusterServiceProfile page
- 31—User is not enabled for EMCC
- 39—Default and Backup TFTP Service is not configured

Cisco Unified Serviceability Alarm Definition Catalog

System/EMAlarmCatalog

Severity

Warning(4)

Routing List

Sys Log

Event Log

Alert Manager

Parameters

Device Name(String)

Login Date/Time(String)

Login UserID(String)

Reason(String)

Recommended Action

Do the following:

Ensure that the user is a valid EMCC user and that user home cluster is added as a EMCC remote cluster (From Unified CM Administration window, go to **System** > **EMCC** > **Remote Cluster** > **Add New**).

Contact remote site administrator to enable user for EMCC (From Unified CM Administration window, go to **User Management** > **End User** > **Select User** > **Enable Extension Mobility Cross Cluster** checkbox).

Contact remote site administrator for adding or freeing EMCC Base Devices (From Unified CM Administration window, go to **Bulk Administration** > **EMCC** > **Insert/Update EMCC**).

Contact remote site administrator to validate the remote cluster setting for this cluster.

Ensure that a bundle of all Tomcat certificates (PKCS12) got imported into the local tomcat-trust keystore (From the OS Administration window, go to **Security** > **Certificate Management**.

ErrorParsingResponseFromPDP

Cisco Unified Communications Manager failed to parse one or multiple optional elements or attributes in the call routing response from the policy decision point.

A routing response was received from the policy decision point (PDP) but Cisco Unified Communications Manager (Unified CM) failed to parse the optional elements in the response. Optional elements may include modified calling numbers or called numbers, call reject or call diversion reasons, and so on. The cause may be a syntax error or missing attributes in the call routing response.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Policy Decision Point(String)

Called Party Number(String)

Calling Party Number(String)

Calling User Id(String)

Request XML Data(String)

Recommended Action

Check if call routing response from the policy decision point complies with the guidelines specified for external call control in the Cisco Unified Communications Manager documentation. Check if any optional elements included as the policy obligations in the call routing response are correctly entered according to the external call control documentation, including any applicable API documentation.

FailedToFulfillDirectiveFromPDP

Cisco Unified Communications Manager cannot fulfill the call routing directive returned by the PDP. The failure can occur because of the following conditions:

- Call was cleared by a CTI application before Cisco Unified Communications Manager was able to route it to the location defined by the PDP.
- Call that was allowed by a policy server was redirected by the CTI application to a destination.
- Annunciator ID was misconfigured in the PDP.
- Unified CM attempted to invoke a media resource such as Annunciator but no resources were available.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning(4)

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

Policy Decision Point(String)

Reason, Unified CM failed to fulfill the directive(String)

Called Party Number(String)

Calling Party Number(String)

Calling User Id(String)

Recommended Action

In many cases, the cause for a failure occurs because of the intervention by a CTI application which scoops up the call before Unified CM is able to fulfill the routing directive in the PDP. Examine the CTI application to ensure that the call is in alerting or connected state before the CTI begins to interact with it.

If the failure is caused by a problem with the annunciator ID, ensure the ID has been accurately configured in the PDP and that it exists in Unified CM Administration.

If the failure was caused by a lack of media resources, try increasing the Annunciator Call Count service parameter in the Cisco IP Voice Media Streaming App service.

H323Stopped

Cisco CallManager is not ready to handle calls for the indicated H323 device.

Cisco Unified Communications Manager (Unified CM) is not ready to handle calls for the indicated H.323 device. This could be due to Unified CM being unable to resolve the gateway name to IP address. For trunks, this alarm should only occur when a system administrator has made a configuration change such as resetting the H.323 trunk. For H.323 clients, this alarm occurrence is normal on lower-priority Unified CM nodes when a high-priority Unified CM node starts.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Following information updated: • Parameters • Enum Definitions for DeviceType

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning (4)

Parameters

Device Name. [String] IP Address [String] Device type. [Optional] [Enum]Device description [Optional]. [String] Remote CallManager Server 1[Optional]. [String] Remote CallManager Server 2[Optional]. [String] Remote CallManager Server 3[Optional]. [String]

Recommended Action

If the service was stopped intentionally, no action is required. Check the domain name system (DNS) configuration for any errors in the gateway name or IP address and correct.

Related Topics

DeviceType Enum Definitions for H323Stopped, on page 275

DeviceType Enum Definitions for H323Stopped

Code	Device Type
61	H323_PHONE
62	H323_GATEWAY
122	GATEKEEPER
125	TRUNK

InvalidSubscription

A message has been received from an IME server that contains a subscription identifier that is not handled by this node

Each node that communicates with a IME server saves a subscription identifier associated with each IME client instance. A IME server has sent a message with a subscription identifier that does not match any of the previously sent subscription identifiers.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

WARNING

Recommended Action

This may be a race condition if the IME client instance has been recently added or deleted. If this error continues, there may be a synchronization issue between this node and the IME server sending this message.

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Subscription Identifier(UInt)

IME Server(String)

InvalidQBEMessage

QBE PDU from application is invalid.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

CTI Connection type(String)

Recommended Action

This alarm indicates that TSP/JTAPI has reported a QBE PDU that cannot be recognized by CTIManager. Contact the support organization for the affected application, install the JTAPI or TSP plugin and restart the application. JTAPI/TSP plugins are available from the Find and List Plugins window in Cisco Unified CM Administration (**Application** > **Plugins**).

IPMAManagerLogout

IPMA Manager Logged out.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Warning (4)

Parameters

Servlet Name [String] Reason [String]

Recommended Action

To relogin the user, click update in the CCMAdmin IPMA Service configuration page for this user.

IPMAStopped

IPMA Application stopped and unloaded from Tomcat.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Warning (4)

Parameters

Servlet Name [String] Reason [String]

Recommended Action

Check if Tomcat service is up.

kANNAudioFileMissing

Announcement file not found. The annunciator was unable to access an announcement audio file. This may be caused by not uploading a custom announcement to each server in the cluster or a locale has not been installed on the server.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

WARNING

Routing List

SDI

Event Log

Sys Log

Parameter(s)

Missing filename(String)

Recommended Action

Upload the custom announcement to the server or install the missing locale package.

kANNAudioUndefinedAnnID

Requested announcement not found. This may be caused by using an incorrect announcement identifier for a custom announcement. Use the Cisco Unified CM Admin to view a list of custom announcement identifiers and verify the correct one is being used.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Error to Warning. • Parameter list removed.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Recommended Action

Add the announcement.

kANNAudioUndefinedLocale

Unknown ANN locale. The requested Locale for an announcement is not installed. For network locale you use the platform CLI interface to run (run sql select * from typecountry where enum = #), #=locale. This will tell you what country locale is being requested.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Error to Warning. • Parameter list is updated.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Locale Type [String]

Recommended Action

Install the locale package or check device settings for an incorrect locale value.

kANNDeviceStartingDefaults

The ANN device configuration was not found. A service parameter for Cisco IP Voice Media Streaming App service related to the ANN device configuration was not found. The system will start with the given default setting.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Informational to Warning. • Parameter list added.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameter(s)

Parameter Name [String]

Value Used [String]

Recommended Action

Review the service parameter settings and configure the ANN device settings properly using the Cisco Unified CM Administration.

kCFBDeviceStartingDefaults

CFB device configuration not found. A service parameter for Cisco IP Voice Media Streaming App service related to the CFB device configuration was not found. The system will use the given default setting.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). • Severity changed from Informational to Warning. • New parameters added: ◦ Parameter Name(String) ◦ Value Used(String)

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameter(s)

Parameter Name(String)

Value Used(String)

Recommended Action

Review the service parameter settings and configure the CFB device settings properly using the Cisco Unified CM Administration.

kChangeNotifyServiceCreationFailed

Database change notification subsystem not starting. The background process to activate database changes has failed to start. Database changes affecting the Cisco IP Voice Media Streaming App service will not automatically take effect.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). • Severity changed from Error to Warning. • Following parameters added: ◦ OS Error Code(Int) ◦ OS Error Description(String)

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameter(s)

OS Error Code(Int)

OS Error Description(String)

Recommended Action

Restart the Cisco IP Voice Media Streaming App service to get the DB notification reenabled.

kChangeNotifyServiceGetEventFailed

Invalid notification event returned by database change notification. The change notification subsystem returned an invalid notification event. The Cisco IP Voice Media Streaming App service will terminate. The SW media devices (ANN, CFB, MOH, MTP) will be temporarily out of service and calls in progress may be dropped.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1) • Severity changed from Error to Warning. • Following parameters added: ◦ OS Error Code(Int) ◦ OS Error Description(String)

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameter(s)

OS Error Code(Int)

OS Error Description(String)

Recommended Action

Check the current status of the Cisco IP Voice Media Streaming App service and monitor for repeated occurrences.

kChangeNotifyServiceRestartFailed

Database change notification restart failure. The change notification subsystem failed to restart.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1) • Severity changed from Error to Warning. • Following parameters added: ◦ OS Error Code(Int) ◦ OS Error Description(String)

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameter(s)

OS Error Code(Int)

OS Error Description(String)

Recommended Action

This service has change notification disabled, it may be reenabled at a later time or restart Cisco IP Voice Media Streaming App service to reenable immediately.

kDeviceDriverError

IP voice media streaming device driver error. The IP voice media streaming device driver returned an error. This may indicate a significant media error or resource shortage.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Error [String]

Recommended Action

Restarting the Cisco IP Voice Media Streaming App service or possibly restarting the server may resolve the error condition.

kDeviceMgrCreateFailed

Device connection manager failed to start. The device controller was unable to start a connection to control device registration with CallManager. This is possibly due to lack of memory.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Device Name [String] Server Name [String]

Recommended Action

Restart the Cisco IP Voice Media Streaming App service or restart the Cisco Unified CM server.

kDeviceMgrOpenReceiveFailedOutOfStreams

Open receive failure. The open receive channel failed. This may indicate a mismatch of media resources between Cisco Unified Call Manager and the Cisco IP Voice Media Streaming App service.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Severity changed from Error to warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Trace Name [String]

Recommended Action

Check the performance monitor counters for resource availability on Cisco Unified CM and on Cisco IP Voice Media Streaming App. Also, you might run the Platform CLI command “Show Media Streams” to identify possible media connection resource leaks. Possibly reset the media device or restart Cisco IP Voice Media Streaming App or restart the Cisco Unified CM server.

kDeviceMgrRegisterKeepAliveResponseError

Cisco Unified Communications Manager not responding. The specified Cisco Unified Communications Manager is not responding to the keepalive messages. The connection with Cisco Unified CM is being terminated and the media device will reregister with another Cisco Unified Call Manager if a secondary is configured. Otherwise, the media device will be unavailable until the device is able to reregister with Cisco Unified CM.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Trace Name [String]

Recommended Action

Cisco Unified Communications Manager may have gone down or is unable to respond. Check status of Cisco Unified CM. The media device should automatically reregister.

kDeviceMgrRegisterWithCallManagerError

Connection error with Cisco Unified Communications Manager. The media device was registered with the specified Cisco Unified Communications Manager and received a socket error or disconnect. This may occur normally when Cisco Unified Communications Manager is stopped.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Trace Name [String]

Recommended Action

No action is required; The media device will reregister.

kDeviceMgrSocketDrvNotifyEvtCreateFailed

This alarm get generated when creating a signaling event for communication with the media streaming kernel driver. It can be caused by memory or system resource shortages.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
8.0(1)	Added Routing List elements. Changed severity level to Warning from Error.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning (4)

Routing List

SDI

Event Log

Sys Log

Parameters

Device Name [String]

Trace Name [String]

OS Error Description [String]

Recommended Action

Restart the Cisco IP Voice Media Streaming App service or restart the Cisco Unified Communications Manager server.

kDeviceMgrSocketNotifyEventCreateFailed

Creation socket event failure. An error was reported when creating a notification event for a socket interface. This may be due to a resource shortage. The media device will remain unavailable.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Device Name [String] Trace Name [String] OS Error Description [String]

Recommended Action

Restart the Cisco IP Voice Media Streaming App service and monitor for reoccurrence or restart the Cisco Unified CM server.

kDeviceMgrStartTransmissionOutOfStreams

Start transmission failure. An error was encountered while starting an RTP transmission audio stream. This may indicate a mismatch of resources between Cisco Unified Communications Manager and Cisco IP Voice Media Streaming App service.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Trace Name [String]

Recommended Action

Check the performance counters for the media resources on Cisco Unified CM and Cisco IP Voice Media Streaming App to determine if there is a resource leak. You should also use the platform CLI command "Show Media Streams" to check for orphaned media RTP connections.

kDeviceMgrThreadxFailed

Creation of thread failure. An error was reported when starting a process for the specified media device. This may be due to a system resource shortage.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). • Severity changed from Error to Warning. • Following parameters added: ◦ OS Error Code[Int] ◦ OS Error Description [String]

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Device Name [String] Trace Name [String] OS Error Code [Int] OS Error Description [String]

Recommended Action

Restart the Cisco IP Voice Media Streaming App service or restart the Cisco Unified CM server to recover from this error.

kFixedInputCodecStreamFailed

Fixed input codec stream initialization failure. Initialization of sound card codec source transcoding process failed. The fixed audio source will not play possibly due to memory or resource shortage.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Error to Warning. • Following parameters removed: ◦ Audio Source ID [ULong] ◦ System error code [ULong]

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Error text [String] Codec Type [String]

Recommended Action

Reset MOH device, or restart Cisco IO Voice Media Streaming App service, or restart server.

kFixedInputCreateControlFailed

Fixed stream control create failure. The audio stream control subsystem for the Fixed MOH audio source failed to start. Audio from the MOH Fixed audio source will not be provided for streaming out. This may be due to resource shortage such as memory or availability of the Fixed MOH audio source device.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). • Severity changed from Error to Warning. • Audio Source ID [ULong] parameter is removed.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Codec Type [String]

Recommended Action

Reset MOH device, if failure continues restart the server. Monitor for errors in trace files and system log.

kFixedInputCreateSoundCardFailed

Fixed stream sound card interface create failure. An error was encountered when starting the interface to access the sound card for providing MOH fixed audio. The audio source will not play possibly due to shortage of memory.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Error to Warning. • Audio Source ID [ULong] parameter is removed.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Codec Type [String]

Recommended Action

Reset MOH device, or restart the Cisco IP Voice Media Streaming App service, or restart the server. Check the system log and possibly the traces for Cisco IP Voice Media Streaming App service.

kFixedInputInitSoundCardFailed

Fixed stream sound card interface initialization failure. Initialization of sound card failed. Fixed audio source will not play possibly due to missing or unconfigured USB sound device.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Error to Warning. • Following parameters are removed: ◦ Audio Source ID [ULong] ◦ System error code [ULong]

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Error text [String] Device name [String]

Recommended Action

Check that the USB sound is installed. Reset MOH device, or restart Cisco IP Voice Media Streaming App service, or restart the server. The system log and traces from Cisco IP Voice Media Streaming App may contain additional information.

kFixedInputTranscoderFailed

Fixed input audio stream transcoder failure. An error was encountered while transcoding audio from the sound card. The audio source will not play possibly due an error accessing the sound card.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Error to Warning. • Following parameters are removed: ◦ Audio Source ID [ULong] ◦ System error code [ULong]

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Error text [String]

Recommended Action

Check that the USB sound device is properly installed. Unplug the USB sound device and replug back into the USB connector. Reset MOH device, restart Cisco IP Voice Media Streaming App service, or restart the server.

kGetFileNameFailed

Get audio source file name failure. The Music-on-Hold audio source is not assigned to an audio file.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). • Severity changed from Error to Warning. • Audio Source ID [ULong] parameter is removed.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

Codec Type [String]

Recommended Action

Assign the audio source to an audio file or change the value of the MOH audio source to a value that has been configured.

kIPVMSMgrEventCreationFailed

Creation of required signaling event failed. An error was encountered when creating a signaling event component. This may be due to a resource shortage. The Cisco IP Voice Media Streaming App service will terminate.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

OS Error Description(String)

Recommended Action

Check the trace files for more information. The service should automatically be restarted. If this error continues to reoccur the server may need to be restarted.

kIPVMSMgrThreadxFailed

Creation of the IPVMSMgr thread failed. An error was encountered while starting a process thread. The Cisco IP Voice Media Streaming App service will terminate. The software media devices (ANN, CFB, MOH, MTP) will be unavailable while the service is stopped.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

OS Error Description(String)

Recommended Action

Monitor the status of the Cisco IP Voice Media Streaming App service. It should automatically be restarted. If the error reoccurs, restart the server.

klpVmsMgrThreadWaitFailed

Error while waiting for asynchronous notifications of events. An error was reported while the primary control process for Cisco IP Voice Media Streaming App was waiting on asynchronous events to be signaled. The service will terminate and should automatically be restarted. This will cause a temporary loss of availability for the software media devices (ANN, CFB, MOH, MTP).

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Recommended Action

Monitor the service and status of the software media devices. The service should automatically restart. If the problem continues, review the trace files for additional information. A server restart may be required if this repeats.

kMOHMgrCreateFailed

Error starting MOH Audio source subcomponent. A error was encountered by the Music-on-Hold device while starting the sub-component that provides audio from files or sound card. This may be due to shortage of resources (memory).

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). • Severity changed from Error to Warning. • OS Error Description(String) parameter is added.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameter(s)

OS Error Description(String)

Recommended Action

Restart the Cisco IP Voice Media Streaming App service or restart the server.

kMOHMgrExitEventCreationFailed

Creation of MOH manager exit event failure. An error was encountered when allocating a signaling event. This may be caused by a resource shortage.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

OS Error Description(String)

Recommended Action

Restart the Cisco IP Voice Media Streaming App service or restart the server.

kMOHMgrThreadxFailed

Starting of MOH audio manager failed. An error was encountered when starting the Music-on-Hold audio manager subcomponent. Music-on-Hold audio services will not be avaliable.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.

Cisco Unified CommunicationsRelease	Action
8.0(1)	This alarm is available in 8.0(1). • Severity changed from Error to Warning. • OS Error Description(String) parameter is added.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Parameters

OS Error Description(String)

Recommended Action

Restart the Cisco IP Voice Media Streaming App service.

kMTPDeviceRecordNotFound

MTP device record not found. A device record for the software media termination point device was not found in the database. This is normally automatically added to the database when a server is added to the database. The software MTP device will be disabled.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Severity changed from Informational to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Recommended Action

If MTP functionality is required, you will need to delete the server and readd the server back to the database using CCMAdmin.

Warning WARNING: This may require many additional configuration settings to be reapplied such as CallManager Groups, Media Resource groups and more.

kRequestedCFBStreamsFailed

CFB requested streams failure. The resources for the number of requested full-duplex streams was not available.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Warning.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

WARNING

Recommended Action

Verify the Cisco IP Voice Media Streaming App service parameter for number of CFB calls. Restart the server to reset the stream resources.

kRequestedMOHStreamsFailed

MOH requested streams failure. The resources for the number of requested streams was not available.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Warning.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

WARNING

Recommended Action

Verify the number of calls configuration setting for Music-on-Hold device. Restart the server to reset the resources.

kRequestedMTPStreamsFailed

MTP requested streams failure. The resources for the number of requested full-duplex Media Termination Point streams was not available.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Warning.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

WARNING

Recommended Action

Verify the Cisco IP Voice Media Streaming App service parameter setting for number of MTP calls is correct. Restart the server to reset the available resources.

LogCollectionJobLimitExceeded

The number of Log Collection Jobs have exceeded the allowed limit. The number of concurrent trace collection from the server has exceeded the allowed limit of trace collection. The allowed limit is defined in the documentation for Trace and Log Central, however this limit can not be changed by sysadmin.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Informational to Warning.

Facility/Sub-Facility

CCM_TCT-LPMTCT

Cisco Unified Serviceability Alarm Definition Catalog

System/LpmTct

Severity

Warning

Parameters

JobType [String]

Recommended Action

Cancel one or more of the currently running queries and try again to configure the trace collection.

LDAPServerUnreachable

Authentication server could not be reached.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	New Alarm for this release.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Warning

Parameters

Message(String)

Recommended Action

Check reachability to Authentication Server.

LogPartitionLowWaterMarkExceeded

The percentage of used disk space in the log partition has exceeded the configured low water mark.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_TCT-LPMTCT

Cisco Unified Serviceability Alarm Definition Catalog

System/LpmTct

Severity

Warning

Parameters

UsedDiskSpace [String] MessageString [Optional]. [String]

Recommended Action

Login into RTMT and check the configured threshold value for LogPartitionLowWaterMarkExceeded alert in Alert Central. If the configured value is set to a lower than the default threshold value unintentionally, change the value to default. Also, examine the trace and log file setting for each of the application in trace configuration page under CCM Serviceability. If the number of configured traces / logs is set to greater than 1000, adjust the trace settings from trace configuration page to default. Also, clean up the trace files that are less than a week old. You can clean up the traces using cli “file delete” or using Remote Browse from RTMT Trace and Log Central function.

MaliciousCall

Malicious Call Identification feature is invoked in Cisco CallManager.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Informational to Warning.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Parameters

Called Party Number [String] Called Device Name [String] Called Display Name [String] Calling Party Number [String] Calling Device Name [String] Calling Display Name [String]

Recommended Action

No action is required.

MaxDevicesPerNodeExceeded

An application has opened more devices than the limit set in the CTIManager service parameter, Maximum Devices Per Node.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiMaxDevicesPerNodeExceeded.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Recommended Action

One or more applications are controlling more devices than the CTI support allows on the specified Unified CM node. Review the application configuration and remove devices that are not required to be controlled. The stability of the system will be impacted if the total number of devices controlled by applications is not properly restricted to the device limit specified by the CTIManager service parameter, Maximum Devices Per Node.

MaxDevicesPerProviderExceeded

An application has opened more devices than the limit set in the CTIManager service parameter, Maximum Devices Per Provider.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiMaxDevicesPerProviderExceeded.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Recommended Action

The application is controlling more devices than the CTI support allows. Review the application configuration and remove devices that are not required to be controlled. The stability of the system will be impacted if the application does not restrict support to the device limit specified by CTI in the CTIManager service parameter, Maximum Devices Per Provider.

MediaResourceListExhausted

The requested device type is not found in the media resource list or default list or the configured devices are not registered.

The requested device is not configured in the Media Resource Group List or Default List, or it's possible that one or more of the devices that are configured in the Media Resource Group List or Default List are not registered to Cisco Unified Communications Manager.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Enum Definitions for MediaResourceType is updated.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning (4)

Parameters

Media Resource Type [Enum]Media Resource List Name [String]

Recommended Action

First, go to Cisco Unified CM Administration to check the configuration of the devices that are part of the Media Resource Groups in the Media Resource Group List that was specified in the alarm (Media Resource Group List Configuration window and Media Resource Group Configuration window in Unified CM Administration).

Check whether the requested type of device is configured in any of the Media Resource Groups in that particular Media Resource Group List in Cisco Unified CM Administration; for RSVP Agent, check whether any media termination point or transcoder is configured in any of the Media Resource Groups in that particular Media Resource Group List. Next, go to the Media Resources menu in Cisco Unified CM Administration to see all the devices of the requested type and then check all the Media Resource Groups (irrespective of whether they

belong to the Media Resource Group List for which the alarm is generated) to see whether the devices belong to at least one Media Resource Group.

If there exists some media resources of the requested type which do not belong to any Media Resource Groups, then these devices will belong to the default list. If the requested type of devices are not configured in any of the Media Resource Groups of the Media Resource Group List for which the alarm is generated or the Default List, add the requested type of device to a Media Resource Group in the specified Media Resource Group List or add it to the Default List.

To add a media resource to the Default List remove the Media Device from all the Media Resource Groups. In general, when a new media device is initially added to Unified CM it will automatically be added to the Default List. This Default List can be used by any device or trunk. But when the media device is added to any particular Media Resource Group it will not be available to the Default List. It can only be used by devices and trunks that are configured with the Media Resource Group List which have that particular Media Resource Group.

Note that a particular Media Resource Group can be added to multiple Media Resource Group Lists. If the requested device is properly configured in Cisco Unified CM Administration, check whether the device is registered to Unified CM. To do that go to the Media Resources menu of the requested type of device (such as Annunciator or Conference Bridge or Media Termination Point or Music On Hold Server or Transcoder) and click the Find button. It will display all the devices of that type with their status, device pool, etc. Check the status field to see whether it is registered with the Cisco Unified CallManager. Note that the display on the status field is not a confirmation that the device is registered to Unified CM. It may happen in a Unified CM cluster that the Publisher can only write to the Unified CM database and suppose the Publisher goes down. Because the Subscriber may not be able to write to the database the devices may still display as registered in Unified CM Administration after they are unregistered. However, if the Publisher is down that should generate another alarm with higher priority than this alarm. If the device is not registered, click on the name of that particular device and check the type of the device.

Device types including Cisco Conference Bridge Software, Cisco Media Termination Point Software, or that specify a server name that is the same name as a Unified CM node of the cluster indicate that the requested device is a software device and is part of the Cisco IP Voice Media Streaming application. Check to be sure that the IP Voice Media Streaming App service is enabled on that Unified CM node (**Cisco Unified Serviceability** > **Tools** > **Service Activation**) and if it is not enabled, activate the Cisco IP Voice Media Streaming App service. Devices should try to register. You can also check the status of the service to be sure it is showing as Started (**Tools** > **Control Center** > **Feature Services**). If the device type is a type other than Cisco Conference Bridge Software, Cisco Media Termination Point Software, or a server name that is the same name as a Unified CM node, that indicates that the device is an external media resource to Unified CM.

Check the configuration (such as Conference Bridge type, MAC address, and conference bridge name in the case of a conference bridge; Media Termination Point name in the case of a Media Termination Point; Transcoder type, MAC address, and Transcoder name in the case of a Transcoder) of the device in Cisco Unified CM Administration and compare it with the configuration of the actual device. To check the configuration of the actual device you may need to refer to the user manual of the media device.

The user manual should provide all the details such as connecting to the media device to check the configuration, commands needed to view and update the configuration, and so on. If configuration in Unified CM and on the actual devices are different, make the necessary changes so that the configurations match. If the configuration matches and the device is still not registered, restart the external media device or the service associated with the external media device. If the external media device continues to fail to register with Unified CM, check the network connectivity between Unified CM and the media device.

Related Topics

MediaResourceType Enum Definitions for MediaResourceListExhausted, on page 309

MediaResourceType Enum Definitions for MediaResourceListExhausted

Code	Definition
1	MediaTerminationPoint
2	Transcoder
3	ConferenceBridge
9	RSVP Agent

MemAllocFailed

CMI tried to allocate memory and failed.

Cisco Unified Communications Manager tried to read the Cisco Messaging Interface service parameters but not enough memory was allocated for the task and so the information could not be read.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Added to CallManager Catalog.

Cisco Unified Serviceability Alarm Definition Catalog

CMIAlarmCatalog/CMI

Severity

WARNING

Routing List

Event Log

SDI

Parameter(s)

Memory Allocation Failure(String)

Recommended Action

Use the Real-Time Monitoring Tool to check the performance counters related to system memory, to learn whether any memory leaks or spikes in CPU are occurring. Correct any anomalous memory issues you find.

If you do not find any issues with memory, collect the system/application event logs and the performance (perfmon) logs and report this alarm to the Cisco Technical Assistance Center (TAC).

MohNoMoreResourcesAvailable

No more MOH resources available.

This alarm occurs when allocation of Music On Hold fails for all the registered MOH servers belonging to the Media Resource Group List and Default List. Each MOH server may fail for different reasons. Following are some of the reasons that could cause an MOH server allocation to fail: All the resources of MOH server are already in use; No matching codecs or capability mismatch between the held party and MOH server; Not enough bandwidth between the held party and MOH source; No audio stream available for the MOH server.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Recommended Action

If all the resources of the MOH servers are already in use, check to be sure that all the MOH servers that belong to the Media Resource Groups of the indicated Media Resource Group List and Default List are configured and registered in all the applicable Unified CM nodes. To check the registration status go to the **Media Resources** > **Music On Hold Server** menu and click the Find button. It will display all the MOH servers with their status, device pool, and so on.

Check the status field to discover whether it is registered with Unified CM. Note that the display on the status field is not a confirmation that the device is registered to Unified CM. It may happen in a Unified CM cluster that the Publisher can only write to the Unified CM database and the Publisher goes down. Because the Subscriber may not be able to write to the database, the devices may still display as registered in Unified CM Administration after they are actually unregistered. However, if the Publisher is down that should generate another alarm with higher priority than this alarm.

The MOH allocation can also fail due to codec mismatch or capability mismatch between the endpoint and the MOH server. If there is a codec mismatch or capability mismatch (such as the endpoint using IPv6 addressing but MOH server supporting only IPv4), an MTP or transcoder should be allocated. If the MTP or transcoder is not allocated then either MediaResourceListExhausted (with Media Resource Type as Media

termination point or transcoder) or MtpNoMoreResourcesAvailable alarm will be generated for the same Media Resource Group List and you should first concentrate on that alarm.

The MOH allocation may even fail after checking the region bandwidth between the regions to which the held party belongs and the region to which the MOH server belongs. Increasing the region bandwidth may be a solution to the problem, but that decision should be made after careful consideration of the amount of bandwidth you're willing to allocate per call between the set of regions.

You'll need to weigh different factors such as the total amount of available bandwidth, the average number of calls, the average number of calls using the MOH servers, approximate bandwidth use per call, and so on, and accordingly calculate the region bandwidth. Another possible cause is that the bandwidth needed for the call may not be available. This can occur if the MOH server and endpoint belong to different locations and the bandwidth that is set between the locations is already in use by other calls.

Examine the bandwidth requirements in your deployment to determine whether bandwidth between the locations can be increased. However, please note that increasing the bandwidth between these two locations means that you may need to reduce the bandwidth between other locations.

Refer to the System Guide, SRNDs, and related Unified CM documentation for more details. Be aware that reducing the bandwidth or removing the higher bandwidth codecs from configuration may result in poor voice quality during call. Consider increasing the total amount of network bandwidth. Another reason for the MOH allocation failure may be due to meeting the maximum number of unicast or multicast streams supported by the MOH server.

If all available streams are already in use, none can be allocated. Finally, check the Music On Hold Audio Source Configuration window in Cisco Unified CM Administration to confirm that at least one audio source is configured. If an audio source is not configured, upload an audio file and then configure the audio source in Cisco Unified CM Administration (refer to the Music On Hold configuration documentation for specific details).

MtpNoMoreResourcesAvailable

Media termination point or transcoder allocation failed.

The alarm occurs when allocation of a media termination point (MTP) or transcoder fails for all the registered MTPs or transcoders belonging to the Media Resource Group List and Default List. Each MTP or transcoder may fail for different reasons. Following are some of the reasons that could cause an MTP or transcoder allocation to fail: a capability mismatch between the device endpoint and MTP/transcoder, codec mismatch between the endpoint and the MTP/transcoder; a lack of available bandwidth between the endpoint and the MTP/transcoder; or because the MTP/transcoders resources are already in use.

A capability mismatch may be due to the MTP/transcoder not supporting one or more of the required capabilities for the call such as Transfer Relay Point (which is needed for QoS or firewall traversal), RFC 2833 DTMF (which is necessary when one side of the call does not support RFC 2833 format for transmitting DTMF digits and the other side must receive the DTMF digits in RFC2833 format, resulting in conversion of the DTMF digits), RFC 2833 DTMF passthrough (in this case, the MTP or transcoder does not need to convert the DTMF digits from one format to another format but it needs to receive DTMF digits from one endpoint and transmit them to the other endpoint without performing any modifications), passthrough (where no codec conversion will occur, meaning the media device will receive media streams in any codec format and transmit them to the other side without performing any codec conversion), IPv4 to IPv6 conversion (when one side of the call supports only IPv4 and the other side of the call supports only IPv6 and so an MTP needs to be inserted to perform the necessary conversion between IPv4 and IPv6 packets), or multimedia capability (if a call involving video and/or data in addition to audio requires insertion of an MTP or transcoder then the MTP/transcoder which supports multimedia will be inserted).

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Error to Warning. • Media Resource List Name parameter added.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Parameter(s)

Media Resource List Name(String)

Recommended Action

If the MTP or transcoder allocation is failing due to a capability mismatch, it's possible that the media device does not support the capability (such as IPv4 to IPv6 conversion, passthrough) or the capability might not be configured in the device. Please check the user guide and documentation of the media device to make sure that device supports all the necessary capabilities. Also, caution should be taken care if all the MTP or transcoders are configured with all the supported capabilities.

There are certain capabilities (such as RFC 2833 DTMF or RFC 2833 DTMF passthrough or passthrough) which could be supported by most of the MTPs or transcoders and there may be certain capabilities (such as IPv4 to IPv6 conversion and vice versa or Transfer Relay Point or multimedia capability) which can be supported by only by a single MTP or transcoder depending on the devices that you have. For example, you may have IP phones that support only IPv4 protocol and there may also be IP phones that support only IPv6 protocol.

To make a call between IPv4-only and IPv6-only phones, you need to have an MTP configured to perform the conversion of IPv4 to IPv6 and vice versa. However, suppose all the MTPs or transcoders are configured with all the supported capabilities and only one MTP supports IPv4 to IPv6 conversion; if this MTP is configured with all the supported capabilities (which all the other MTPs or transcoders in the same MRGL or default MRGL also support) it may happen that this MTP can get allocated for Transfer Relay Point or RFC 2833 DTMF or RFC 2833 DTMF passthrough or passthrough instead. As a result, when the need arises for IPv4 to IPv6 conversion (which other MTPs or transcoders in the same MRGL or default MRGL do not support), all the resources of MTP may be in use and the IPv4 to IPv6 conversion may fail. To avoid this kind of problem, setting the priority of the media resources may be a good idea.

This can be done only in the Media Resource Group List and not in the Default List of the media resources. In any Media Resource Group List all the Media Resource Groups have different priorities; during allocation the first Media Resource Group is always checked for availability of the requested type of the media devices.

The first Media Resource Group in the Media Resource Group List will have the highest priority, then the second one, and so on.

To check all the Media Resource Groups and their priority go the Media Resources and Media Resource Group List of Cisco Unified CM Administration page and click the appropriate Media Resource Group List and check the Selected Media Resource Groups; the priority decreases from top to bottom. So, the MTP or transcoder that you want to be selected for the most basic functionalities should be positioned in the higher priority Media Resource Groups whereas the ones with more rare functionality should be positioned in the Media Resource Groups with lower priority. MTP/transcoder allocation may fail due to codec mismatch between the endpoint and the MTP/transcoder.

A solution may be to configure the MTP/transcoder with all the supported codecs (as specified in the user guide of the MTP/transcoder), but be aware that doing so might result in too much bandwidth being allocated for calls. You'll need to weigh different factors such as the total amount of available bandwidth, the average number of calls, approximate bandwidth use per call (not involving MTP/transcoder), and so on, and accordingly calculate the maximum bandwidth that can be allocated per call involving an MTP/transcoder and take that into consideration when configuring the supported codecs in the MTPs and transcoders. A good idea is to configure the media devices with all the supported codecs and set the region bandwidths to restrict too much bandwidth usage (refer to the Unified CM documentation for details on region and location settings).

Also, there may be a codec mismatch between the endpoint and the MTP/transcoders after considering the region bandwidth between the MTP/transcoder and the endpoint. Increasing the region bandwidth may be a solution to the problem, but again, that decision should be made after careful consideration of the amount of bandwidth you're willing to allocate per call between the set of regions. Another possible cause that an MTP/transcoder did not get allocated is because there was not enough available bandwidth for the call.

This can happen if the MTP/transcoder and endpoint belong to different locations and the bandwidth that is set between the locations is already in use by other calls. Examine the bandwidth requirements in your deployment to determine whether bandwidth between the locations can be increased.

However, please note that increasing the bandwidth between these two locations means that you may need to reduce the bandwidth between other locations. Refer to the System Guide, SRNDs, and related Unified CM documentation for more details. Be aware that reducing the bandwidth or removing the higher bandwidth codecs from configuration may result in poor voice quality during call. Consider increasing the total amount of network bandwidth available. Finally, if MTP or transcoder allocation fails due to capability mismatch or all the resources being in use, consider installing additional MTP or transcoder devices.

MTPDeviceRecoveryCreateFailed

MTP device recovery create failure. An error was encountered trying to restart the Media Termination Point device. This may be due to a shortage of application memory.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Changed severity level from Error to Warning and added existing Routing List elements and Parameters.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Routing List

SDI

Event Log

Sys Log

Parameters

OS Error Description(String)

Recommended Action

Restart the IP Voice Media Streaming App service or restart the server.

NotEnoughChans

Call attempt was rejected because requested gateway channel(s) could not be allocated. Some of the more common reasons for the lack of channel to place outgoing calls include: High call traffic volume that has the B-channels in the device fully utilized; B-channels have gone out of service for the following reasons: Taking the channel out of service intentionally to perform maintenance on either the near- or far-end; MGCP gateway returns an error code 501 or 510 for a MGCP command sent from Cisco Unified Communications Manager; MGCP gateway doesn't respond to an MGCP command sent by Unified CM three times; a speed and duplex mismatch exists on the Ethernet port between Unified CM and the MGCP gateway.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Error to Warning. • Device Name(String) is the only parameter

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Parameters

Device Name(String)

Recommended Action

Add more gateway resources; Check the Unified CM advanced service parameter, Change B-channel Maintenance Status to determine if the B-channel has been taken out of service intentionally; Check the Q.931 trace for PRI SERVICE message to determine whether a PSTN provider has taken the B-channel out of service; Reset the MGCP gateway; Check the speed and duplex settings on the Ethernet port.

NoCallManagerFound

No Cisco Unified Communications Manager (Cisco Unified CM, formerly known as Cisco Unified CallManager) node has been configured. A Cisco Unified Communications Manager Group exists but it has no Cisco Unified CM node configured as its group member.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kNoCallManagerFound.
8.0(1)	Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Warning

Parameters

Error [String]

Recommended Action

In Cisco Unified CM Administration (**System** > **Cisco Unified CM Group**), configure at least one Cisco Unified CM node for the Cisco Unified CM Group referenced in this alarm. The Cisco Unified CM Group is part of the device pool to which the specified phone belongs.

OutOfRangeMohAudioSource

The Music On Hold (MOH) audio source ID is invalid. This alarm occurs when Music On Hold fails because the MOH audio source ID that is requested is not within the valid range of 1 to <*maximum value parameter in this alarm*>. The caller will hear Tone On Hold instead of the desired Music On Hold audio.

History

Cisco Unified Communications Release	Action
10.0(1)	Error message added.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning (4)

Routing List

SDL

SDI

Sys Log

Event Log

SNMP Traps

Data Collector

Alert Manager

Parameters

MohAudioSourceId

MaxMohAudioSourceId

Recommended Action

If the MOH audio source ID was provided as part of the MOH Audio Source override header ("X-cisco-moh-source: #,#") from an incoming call over the SIP trunk, then the value must be corrected at the source of this header. Otherwise, check the values for the MOH audio source in the CallManager service parameter settings or possibly other configuration settings that are related to the party that initiated the hold.

PublishFailed

Publish Failed.

Unified CM attempted to store a number into the IME distributed cache, but the attempt failed. This is typically due to a transient problem in the IME distributed cache. The problem will self-repair under normal conditions. However, you should be aware that, as a consequence of this failure, the E.164 DID listed as part of the alarm will not be present in the IME distributed cache for a brief interval. Consequently, this may delay the amount of time until which you will receive VoIP calls made to that number - they may continue over the PSTN for some callers. It is useful to be aware of this, in case you are trying to understand why a call is not being made over VoIP.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

WARNING

Recommended Action

If you notice single small numbers of these alarms in isolation, no action is required on your part. However, a large number of them indicates a problem in the IME distributed cache, most likely due to problems with Internet connectivity. Check your Internet connectivity.

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

DID(String)

QRTRequest

User submitted problem report using Quality Report Tool. User has experienced a problem with Phone and has submitted problem report.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Changed Data Collector Routing List element to Alert Manager.

Facility/Sub-Facility

CCM_CBB-CALLBACK

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CEF

Severity

Warning (4)

Routing List

SDI

Sys Log

Event Log

Alert Manager

SNMP Traps

Parameters

Category(String)

Reason Code(String)

Report Timestamp(String)

Device name.(String)

Device IP address.(String)

Directory number(String)

Recommended Action

Investigate the cause for problem report.

RejectedRoutes

Rejected route due to Untrusted status.

This alarm is generated when Unified CM learned a route from the IME server. However, due to the configured Trusted or Untrusted list, the route was rejected.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

WARNING_ALARM

Recommended Action

This condition is not an error. However, it indicates to you that one of your users called a number which was reachable over IME, however, due to your configured Trusted or Untrusted list, a IME call will not be made. You might wish to consider adding the domain or prefix to your Trusted list or removing it from the Untrusted list.

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Domain name(String)

Phone number(String)

RouteListExhausted

An available route could not be found in the indicated route list. This alarm is generated when all members' status is unavailable or busy or when the member is down (out of service), not registered, or busy.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning (4)

Parameters

Route List Name [String]

Recommended Action

Consider adding additional routes in the indicated route list. For shared line when some phones are not ringing, check the busy trigger and maximum call settings of shared line phones; check whether there are some outstanding calls on that DN.

When one shared line phone answers an incoming call, the other shared line phone cannot see that remote-in-use call; check the privacy setting of the phone that answers the call.

Try to make a call directly to the member, bypassing the route list, to verify that there is not a device or connectivity issue. If you cannot identify the cause through these steps, gather the CCM (SDI) trace and contact the Cisco Technical Assistance Center; TAC may be able to locate a cause code which may provide additional explanation for this alarm.

ServiceStartupFailed

Service startup failure.

Cisco Unified Serviceability Alarm Definition Catalog

System/Generic

Severity

Warning (4)

Parameters

None

Recommended Action

Restart the service.

ServingFileWarning

There was an error during processing of file request. This could happen if the requested file is not found by the server, or other error indicated by the “Reason” clause when processing the file request.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Name changed from kServingFileWarning.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Warning (4)

Parameters

ErrorNumber [Int] FileName [String] IPAddress_Port [String] Mode [String] OpCode [Int] Reason [String]

Recommended Action

You can safely ignore this alarm if the reason shown in this alarm is “File not found” and if that file is the MAC address-based file name for a phone that you are auto-registering; in that case, the phone is not yet registered with the database and so it is normal for the phone's file not be found. In the case that auto-registration is disabled, this alarm shows that the phone or device is not added to Cisco Unified Communications Manager (Cisco Unified CM). Either add the phone to Cisco Unified CM or remove the phone from the network. If you still get this error after removing the phone(s), go to Cisco Unified Serviceability and enable Detailed

level traces in the Trace Configuration window for the TFTP service and contact the Cisco Technical Assistance Center (TAC).

SparePartitionHighWaterMarkExceeded

The percentage of used disk space in the spare partition has exceeded the configured high water mark. Some of the trace files will be purged until the percentage of used disk space in the spare partition gets below the configured low water mark.

Note Spare Partition is not used for Intercompany Media Engine server. So this alert will not be triggered for Intercompany Media Engine.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.
8.0(1)	Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_TCT-LPMTCT

Cisco Unified Serviceability Alarm Definition Catalog

System/LpmTct

Severity

Warning

Parameters

UsedDiskSpace [String] MessageString [Optional]. [String]

Recommended Action

Login into RTMT and cheek the configured threshold value for SparePartitionHighWaterMarkExceeded alert in Alert Central. If the configured value is set to a lower than the default threshold value unintentionally, change the value to default.

If you continue to receive this alert for half an hour after receiving the 1st alert, check for the disk usage for Spare partition under “Disk Usage” tab in RTMT. If the disk usage shown under that tab is higher than configured value in SparePartitionLowWaterMarkExceeded alert configuration, contact Cisco TAC to troubleshoot the cause of high disk usage in Common partition.

SSOuserNotInDB

User not found in database.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	New alarm for this release.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Parameters

Message(String)

Recommended Action

Perform sync manually or wait till next scheduled next sync.

SIPStopped

Cisco CallManager is not ready to handle calls for the indicated SIP device. Possible reasons could be internal database error, the SIP device is not activated on this node, the SIP device failed to register or the SIP device was deleted from admin page.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Enum Definitions for InTransportType and OutTransportType are updated. Recommended Action changed.
7.0(1)	IPV6Address parameter added.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning (4)

Parameters

Device Name. [String] IP Address [String] Device type. [Optional] [Enum]Device description [Optional]. [String] Incoming Port Number. [UInt] Outgoing Port Number. [UInt] Incoming Transport Type [Enum]Outgoing Transport Type [Enum]IPV6Address [Optional]. [String]

See the following:

Recommended Action

This alarm doesn't necessarily mean an error. It could occur as a result of normal administrative changes. If the alarm is unexpected, check whether the StationPortInitError alarm also fired. Check the Device Pool assigned to the SIP device identified in this alarm to ensure that the Cisco Unified Communications Manager Group of the Device Pool includes the Unified CM node that issued the alarm.

Related Topics

DeviceType Enum Definitions for SIPStopped, on page 323
InTransportType Enum Definitions for SIPStopped, on page 323
OutTransportType Enum Definitions for SIPStopped, on page 324

DeviceType Enum Definitions for SIPStopped

131—SIP_TRUNK

InTransportType Enum Definitions for SIPStopped

Code	Definition
1	TCP
2	UDP
3	TLS
4	TCP/UDP

OutTransportType Enum Definitions for SIPStopped

Code	Definition
1	TCP
2	UDP
3	TLS

SIPLineRegistrationError

A SIP line attempted to register with CallManager and failed due to the error indicated in the Reason Code parameter. The alarm could indicate a device misconfiguration, database error, or an illegal/unknown device trying to attempt a connection.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Error to Warning. • Enum Definitions for DeviceType are updated. • Enum Reasons table is updated.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Parameters

Device IP address. [String] Device Port. [UInt] Device name [Optional]. [String] Device MAC address [Optional]. [String] Device type. [Optional] [Enum]Reason Code [Optional]. [Enum]Connecting Port [UInt] Configured DNs. [String] Registering SIP User. [String]

Recommended Action

Verify that the directory number(s) on the device itself match the directory number(s) that are configured for that device in Cisco Unified CM Administration. Also, confirm that database replication is working. Refer to the reason code definitions for additional recommended actions.

Related Topics

DeviceType Enum Definitions for SIPLineRegistrationError, on page 325
Reason Code Enum Definitions for SIPLineRegistrationError, on page 327

DeviceType Enum Definitions for SIPLineRegistrationError

Code	Device Type
1	CISCO_30SP+
2	CISCO_12SP+
3	CISCO_12SP
4	CISCO_12S
5	CISCO_30VIP
6	CISCO_7910
7	CISCO_7960
8	CISCO_7940
9	CISCO_7935
12	CISCO_ATA_186
20	SCCP_PHONE
61	H323_PHONE
72	CTI_PORT
115	CISCO_7941
119	CISCO_7971
255	UNKNOWN
302	CISCO_7989
307	CISCO_7911

Code	Device Type
308	CISCO_7941G_GE
309	CISCO_7961G_GE
335	MOTOROLA_CN622
336	BASIC_3RD_PARTY_SIP_DEVICE
348	CISCO_7931
358	CISCO_UNIFIED_COMMUNICATOR
365	CISCO_7921
369	CISCO_7906
374	ADVANCED_3RD_PARTY_SIP_DEVICE
375	CISCO_TELEPRESENCE
404	CISCO_7962
412	CISCO_3951
431	CISCO_7937
434	CISCO_7942
435	CISCO_7945
436	CISCO_7965
437	CISCO_7975
446	CISCO_3911
468	CISCO_UNIFIED_MOBILE_COMMUNICATOR
478	CISCO_TELEPRESENCE_1000
479	CISCO_TELEPRESENCE_3000
480	CISCO_TELEPRESENCE_3200
481	CISCO_TELEPRESENCE_500
484	CISCO_7925

Code	Device Type
493	CISCO_9971
495	CISCO_6921
496	CISCO_6941
497	CISCO_6961
20000	CISCO_7905
30002	CISCO_7920
30006	CISCO_7970
30007	CISCO_7912
30008	CISCO_7902
30016	CISCO_IP_COMMUNICATOR
30018	CISCO_7961
30019	CISCO_7936
30035	IP_STE

Reason Code Enum Definitions for SIPLineRegistrationError

Code	Reason
2	MisconfiguredDirectoryNumber - There is a configuration mismatch between the directory numbers configured on the phone and the directory numbers configured in the Cisco Unified CM database. If this is a third-party phone, confirm that the phone configuration is correct and matches the Cisco Unified CM configuration. If this is a Cisco IP phone, confirm database replication has a “good status” in the Unified CM Database Status report. This can be found on the Cisco Unified Reporting web page. If the database replication status is good, reset the device. If the problem still persists, restart the TFTP service and the Cisco Unified CM service from the Control Center - Feature Services web page.
3	MalformedRegisterMessage - Cisco Unified CM cannot process a REGISTER message because of a problem with the format of the message. If the device is a third-party phone, confirm that the endpoint is sending a properly formatted REGISTER message.

Code	Reason
4	AuthenticationError - The digest userid or password sent from the phone does not match the userid or password configured in Cisco Unified CM. Digest userid is the end-user associated with the phone on the Phone Config page, Digest User drop down box. Password is configured on the end user page, digest credentials box. If this is a third-party phone, ensure the phone digest credentials match the digest credentials configured on the End User web page. If this is a Cisco IP phone, confirm database replication has a "good status" in the Unified CM Database Status report. This can be found on the Cisco Unified Reporting web page. If the database replication status is good, reset the device. If the problem still persists, restart the TFTP service and the Cisco Unified CM service from the Control Center - Feature Services web page.
6	MaxLinesExceeded - The phone is attempting to register more lines than are allowed. The maximum lines per device is 1024. Reduce the number of lines configured on this device.
7	TransportProtocolMismatch - Incorrect transport protocol (UDP, TCP or TCL) on which the REGISTER message was received. If the device is a third-party phone, ensure that the phone is using a transport protocol that matches the Phone Security Profile assigned to the phone in the CCMAdmin device page. If the device is a Cisco phone, confirm database replication has a "good status" in the Unified CM Database Status report. This can be found on the Cisco Unified Reporting web page. If the database replication status is good, reset the device. If the problem still persists, restart the TFTP service and the Cisco Unified CM service from the Control Center - Feature Services web page.
8	BulkRegistrationError - A unexpected bulk registration message was received. If this occurs repeatedly, collect SDL/SDI detailed traces with "Enable SIP Keep Alive (REGISTER Refresh) Trace" under Cisco CallManager services turned on and contact TAC.

SIPTrunkPartiallyISV

Some of the remote peers are not available to handle calls for this SIP Trunk.

The alarm provides a list of available remote peers and a list of unavailable remote peers, where each peer is separated by semicolon. For each available peer, the alarm provides resolved IP address and port number, and hostname or SRV (if configured on SIP trunk). For each unavailable peer, the alarm provides the hostname or SRV (if configured on SIP trunk), resolved IP address, port number, and reason code in the following format: ReasonCodeType=ReasonCode.

The ReasonCodeType depends on a SIP response from remote peer as defined in SIP RFCs (Remote), or depends on a reason code provided by Unified CM (Local).

The examples of possible reason codes include:

- Remote = 503 ("503 Service Unavailable" a standard SIP RFC error code)

- Remote = 408 (“408 Request Timeout” a standard SIP RFC error code)
- Local = 1 (“Request Timeout”)
- Local = 2 (local SIP stack is unable to create a socket connection with remote peer)
- Local = 3 (DNS query failed)

  For Local=3, IP address in the alarm is represented as zero, and when DNS SRV is configured on SIP trunk then port is represented as zero.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	• New alarm for this release.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

SIP Trunk Name(String)

Unavailable remote peers with Reason Code(String)

Available remote peers for this SIP trunk(String)

Recommended Action

The available peer list is for notification purposes only; no action is required. For unavailable peers, the following corrective action should be taken.

- For Remote = 503, the possible reasons are:

- Route/SIP trunk for originating side does not exist on remote peer. If remote peer is Unified CM, add a new SIP trunk in Unified CM Administration for the remote peer (**Device** > **Trunk**) and ensure the Destination Address and Destination Port fields are configured to point to the originating host (the originating host is the same node on which this alarm was generated). Also ensure the new SIP trunk has the incoming port in associated SIP Trunk Security Profile configured to be the same as originating side SIP Trunk destination port.
- Route/SIP trunk for originating side does exist on remote peer but port is either used for SIP phone or other SIP trunk. If remote peer is Unified CM, in the Unified CM Administration for the remote peer (**Device** > **Trunk**), ensure the incoming port in associated SIP Trunk Security Profile is configured to be same as originating side SIP Trunk destination port.
- Remote peer has limited resources to handle new calls. If remote peer is administered by a different system administrator, communicate the resource issue with the other administrator.

- For Remote = 408, the possible reason includes:
  - Remote peer has limited resources to handle new calls. If remote peer is administered by a different system administrator, communicate the resource issue with the other administrator.

- For Local = 1, the possible reason could be that no responses are received for OPTIONS request after all retries, when UDP transport is configured in SIP Trunk Security Profile assigned to the SIP trunk on originating side.

  To fix this issue, perform the following steps:
  - If remote peer is Unified CM, in the remote peer Serviceability application, choose Tools > Control Center (Feature Services) and ensure the Cisco CallManager service is activated and started.
  - In the Unified CM Administration for the remote peer, choose **Device** > **Trunk**, and ensure the SIP trunk exists with the incoming port in associated SIP Trunk Security Profile configured to be same as originating side SIP Trunk destination port.
  - Check the network connectivity by using the CLI command utils network ping <remote peer> at the originating side.

- For Local = 2, the possible reason could be that Unified CM is unable to create the socket connection with remote peer.

  To fix this issue, perform the following steps:
  - If remote peer is Unified CM, in the remote peer Serviceability application, choose **Tools** > **Control Center** (Feature Services) and ensure the Cisco CallManager service is activated and started.
  - In the Unified CM Administration for the remote peer, choose **Device** > **Trunk**, and ensure the SIP trunk exists with the incoming port in associated SIP Trunk Security Profile configured to be same as originating side SIP Trunk destination port.
  - Check the network connectivity by using the CLI command utils network ping <remote peer> at the originating side.

- For Local = 3, the possible reason could be that DNS server is not reachable, or DNS is not properly configured to resolve the hostname or SRV which is configured on the local SIP trunk.

  To fix this issue, perform the following steps:

- In the OS Administration, choose **Show** > **Network**, and verify that the DNS Details are correct. If it is not correct, then configure the correct DNS server information by using the CLI command set network dns primary.
- Check the network connectivity with DNS server by using the CLI command utils network ping <remote peer>, and ensure the DNS server is properly configured.

SoftwareLicenseNotValid

There is no valid software license; the Cisco IP Voice Media Streaming App service requires a valid software license to operate.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Warning.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning

Routing List

SDI

Event Log

Sys Log

Recommended Action

Install a valid software license and restart Cisco IP Voice Media Streaming App service.

StationEventAlert

A station device sent an alert to Cisco Unified Communications Manager, which acts as a conduit from the device to generate this alarm.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Warning.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Parameters

Protocol [String] TCP ProcessID [String] Device Text [String] Param1 [UInt] Param2 [UInt]

Recommended Action

Refer to the specific device type and information passed via this alarm to determine the appropriate action.

TestAlarmWarning

Testing warning alarm.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Test

Severity

Warning (4)

Recommended Action

None

TotalProcessesAndThreadsExceededThresholdStart

The current total number of processes and threads has exceeded the maximum number of tasks configured for Cisco RIS Data Collector service parameter. This situation could indicate some process is leaking or some process has thread leaking.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/System Access

Severity

Warning (4)

Parameters

NumberOfProcesses [String] NumberOfThreads [String] Reason [String] ProcessWithMostInstances [String] ProcessWithMostThreads [String]

Recommended Action

Check the Cisco RIS Data Collector service parameter, Maximum Number of Processes and Threads, to see if the parameter has been set to a low value. If it has been, set the value higher or use the default value. Another possible action is that when a new Cisco product is integrated into Cisco Unified Communications Manager (Cisco Unified CM), new processes or threads are added to the system. Even in the normal process load situation, it's possible that the total number of processes and threads has exceeded the configured or default value of the Cisco RIS Data Collector service parameter, Maximum Number of Processes and Threads. Set that parameter to the maximum allowed value.

You can also review the details of this alarm to check the ProcessWithMostThreads description and the ProcessWithMostInstances description to discover which processes have the most threads and the most instances. Determine whether these values are reasonable for this process; if not, contact the owner of the process for troubleshooting the reasons why the thread count or the number of process instances is so high. It is also possible that Cisco RIS Data Collector sent a false alarm, which would indicate a defect in the Cisco RIS Data Collector service.

To determine if this is the cause of the alarm - after you have checked all the other errors described here - use RTMT to check the System object for performance counters Total Threads and Total Processes to confirm that the values in those counters do not exceed the value configured in the Cisco RIS Data Collector service parameter, Maximum Number of Processes and Threads. If the counters do not show a value that is higher than what is configured in the service parameter, restart Cisco RIS Data Collector service. If the alarm persists after restarting the service, go to Cisco Unified Serviceability and collect trace logs (**Trace** > **Configuration**) for Cisco Syslog, Cisco RIS Data Collector, Cisco AMC Service, and Cisco RIS Perfmon Logs and contact Cisco Technical Assistance Center (TAC) for detailed assistance.

ThreadKillingError

An error occurred when CMI tried to stop the CMI service.

As a normal part of the process of stopping the CMI service, open threads are closed (killed). This alarm indicates that a timeout has occurred which means that the shutdown process is taking longer than expected, causing the operating system to return an error.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kThreadKillingError. Enum Definitions for MediaResourceType is updated.

Cisco Unified Serviceability Alarm Definition Catalog

CMIAlarmCatalog/CMI

Severity

WARNING

Routing List

Event Log

SDI

Parameter(s)

Error Information(String)

Recommended Action

Try restarting the CMI service. If the problem persists, collect the system/application event logs and the performance (perfmon) logs and report to Cisco Technical Assistance Center (TAC).

UnableToSetorResetMWI

An error occurred when setting the message waiting indication (MWI) lamp

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

WARNING

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Directory Number(String)

Recommended Action

The line issuing the request to set the MWI lamp on the target line might not have the proper partitions/calling search space settings to allow it to reach the target line. Check the partitions and calling search space of the line that is requesting to set MWI on the target line. The target line should be able to receive a call from the line that is attempting to set MWI.

UnprovisionedMohAudioSource

The Music On Hold (MOH) audio source ID is not provisioned. This alarm occurs when Music On Hold fails because the MOH audio source ID that is requested has not been provisioned by associating the ID# to an audio source file. The caller will hear Tone On Hold instead of the desired Music On Hold audio.

History

Cisco Unified Communications Release	Action
10.0(1)	Error message added.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning (4)

Routing List

SDL

SDI

Sys Log

Event Log

SNMP Traps

Data Collector

Alert Manager

Parameters

MohAudioSourceId

Recommended Action

Check the Music On Hold Audio Source list within Cisco Unified CM Administration to ensure that it has been assigned (provisioned) to an audio wav file, or if ID# 51 is being used, check that the MOH Fixed Audio source has been enabled.

Audio files must be uploaded using the Cisco Unified CM Administration page of each MOH server in the cluster before that server can play the audio file.

UserInputFailure

EMCC login failure due to invalid user input due to invalid user credentials or the credentials have expired. Reason Code: 2—Authentication Error.

Cisco Unified Serviceability Alarm Definition Catalog

System/EMAlarmCatalog

Severity

Warning(4)

Routing List

Sys Log

Event Log

Alert Manager

Parameters

Device Name(String)

Login Date/Time(String)

Login UserID(String)

Reason(String)

Recommended Action

Try again with valid credentials or try resetting the credentials.

UserUserPrecedenceAlarm

User-to-user IE was not successfully tunneled to destination; please refer to reason code for additional details.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Error to Warning. • Enum definitions updated.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning

Parameters

Device Name. [String] Reason Code [Enum]

Recommended Action

For HopCountExceeded alarm, the recommended action is to check that no routing loops exist across the Unified CM trunk interfaces (PRI, intercluster trunk, and so on) and gateway (H.323) devices related to the indicated failed call. By examining trace files and CDR data in all Unified CM nodes and route patterns in gateways (H.323) that are involved in routing of the indicated failed call, you may be able to detect a translation pattern, route list or other routing mechanism that is part of the loop.

Update the routing mechanism that resulted in the loop, and then if the looping route pattern was on a Unified CM, reset the affected route list/pattern in an attempt to clear the route loop; if that fails, reset the affected trunk/gateway or if the looping route pattern was on a H.323 gateway, restart the gateway. For call failure reason UserUserIEDropped, if the indicated device is an H.323 intercluster trunk then the recommended action is to verify that the Passing Precedence Level Through UUIE checkbox has been enabled on the Trunk Configuration window. If the indicated device is an MGCP gateway with Device Protocol set to Digital Access PRI and Passing Precedence Level Through UUIE is enabled on the gateway, then verify that the far-end side of the configured PRI trunk interface supports PRI 4ESS UUIE-based MLPP and sends the UUIE message with IEID value set to USER_USER_IE (126) and the User specific protocol ID value set to PRI_4ESS_UUIE_DEFAULT_PROT_DISC (0x00).

Related Topics

Enum Definitions for UserUserPrecedenceAlarm, on page 338

Enum Definitions for UserUserPrecedenceAlarm

Code	Definition
2	HopCountExceeded—The hop count field in passing User-to-User IE exceeded the maximum value of 10. The reason could be the presence of routing loops across the Unified CM trunk interfaces (PRI, intercluster trunk, and so on). The recommended action is to check that no routing loops exist across the Unified CM trunk interfaces (PRI, intercluster trunk, and so on) and gateway (H.323) devices related to the indicated failed call. By examining trace files and CDR data in all Unified CM nodes and route patterns in gateways (H.323) that are involved in routing of the indicated failed call, you may be able to detect a translation pattern, route list or other routing mechanism that is part of the loop. Update the routing mechanism that resulted in the loop, and then if the looping route pattern was on a Unified CM, reset the affected route list/pattern in an attempt to clear the route loop; if that fails, reset the affected trunk/gateway or if the looping route pattern was on an H.323 gateway, restart the gateway.
3	UserUserIEDropped—The passing UserUserIE is dropped. If the indicated device is an H.323 intercluster trunk then the possible reason could be that the Passing Precedence Level Through UUIE checkbox in the Trunk Configuration window in Unified CM is not enabled; the recommended action is to verify that the Passing Precedence Level Through UUIE checkbox has been enabled. If the indicated device is an MGCP gateway with Device Protocol set to Digital Access PRI, the possible reason could be that in the incoming UUIE message, either the IEID is not set to USER_USER_IE (126) or the User specific protocol ID value is not set to PRI_4ESS_UUIE_DEFAULT_PROT_DISC (0x00); the recommended action is to verify that the far-end side of the configured PRI trunk interface supports PRI 4ESS UUIE-based MLPP and sends the UUIE message with IEID value set to USER_USER_IE (126) and the User specific protocol ID value is set to PRI_4ESS_UUIE_DEFAULT_PROT_DISC (0x00).

BeginThrottlingCallListBLFSubscriptions

Cisco Unified Communications Manager has initiated throttling of CallList BLF Subscriptions as a preventive measure to avoid overloading the system. This alarm is raised when the total number of active BLF subscriptions exceeds the configured limit set by the Presence Subscription Throttling Threshold service parameter.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Warning (4)

Parameters

Active External Presence Subscriptions [UInt] CallList BLF Subscriptions Throttling Threshold [UInt] CallList BLF Subscriptions Resume Threshold [UInt] Total Begin Throttling CallList BLF Subscriptions [UInt]

Recommended Action

Determine if CPU and memory resources are available to meet the higher demand for CallList BLF Subscriptions. If so, increase the CallListBLFSubscriptionsThrottlingThreshold and correspondingly the CallListBLFSubscriptionsResumeThreshold. If not, increase system resources to meet the demand.

kANNAudioCreateDirFailed

Unable to create a subdirectory to contain announcement files. This may be caused by insufficient disk storage. Announcements may not play correctly as a result of this error.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Added more Recommended Action text. Updated parameters and changed severity level from Error to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning (4)

Parameters

OS Error Text(String)

Path Name(String)

Recommended Action

Check for available free space on the common data storage area. If full, take action to remove old trace files to free space. Restart the Cisco IP Voice Media Streaming App service.

MOHDeviceRecoveryCreateFailed

An error got triggered restarting the Music On Hold (MOH) device. It may have been caused by a shortage of memory resources.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Changed severity level from Error to Warning and added existing Routing List elements.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning (4)

Routing List

SDI

Event Log

Sys Log

Parameters

ErrorText(String)

Error(ULong0

Recommended Action

Check the status of the MOH device. If it is not registered and available, restart the Cisco IP voice Media Streaming App service or restart the server.

kDeviceMgrExitEventCreationFailed

Creation of device manager exit event failure. An error was reported when allocating an exit-control event for a SW media device. The device will not be registered with CallManager or active.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
8.0(1)	Added Routing List elements. Changed severity level from Error to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning (4)

Routing List

SDI

Event Log

Sys Log

Parameters

Device Name [String]

Trace Name [String]

OS Error Text [String]

Recommended Action

This error may be due to a memory resource shortage. Restart the Cisco IP Voice Media Streaming App service or restart the Cisco Unified CM server.

kMOHDeviceRecordNotFound

MOH device was not found for the server. This device gets added automatically when a server gets added to the configuration.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
8.0(1)	Updated the descriptive text and Recommended Action text. Added Caution statement. Changed severity level from Informational to Warning.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning (4)

Recommended Action

If MOH functionality is required, you will have to remove and readd the device to database.

Caution Adding and removing the device may impact other configuration settings, for example, Cisco Unified Communications Manager groups and media resource groups.

kMOHBadMulticastIP

An invalid multicast IP address (out of range) was found.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
8.0(1)	Added Routing List elements and changed severity level to Warning from Error. Following parameters are removed: • Audio Source ID [ULong] • Call/Conference ID [ULong] • Multicast IP Port [ULong]

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Warning (4)

Routing List

SDI

Event Log

Sys Log

Parameters

Codec Type [String]

Multicast IP Address [String]

Recommended Action

Correct the setting on the Music-on-Hold device configuration for multicast address.

SSODisabled

Single Sign On (SSO) disabled on Cisco Unified CM.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	New alarm added for this release.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Warning

Parameters

Message(String)

Recommended Action

Run CLI command to enable SSO.

SSONullTicket

A null ticket was passed.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	New alarm added for this release.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Warning

Parameters

Message(String)

Recommended Action

Get non null ticket and retry.

SSOServerUnreachable

SSO server could not be reached.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	New alarm added for this release.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Warning

Parameters

Message(String)

Recommended Action

Check reachability to SSO server.

WDStopped

WebDialer application stopped and was unloaded from Tomcat.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Alert to Warning.

Facility/Sub-Facility

CCM_JAVA_APPS_TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Warning

Parameters

Servlet Name [String] Reason [String]

Recommended Action

Check if Tomcat service is up.

Notice-Level Alarms

The notice-level alarm is 5 and no action is needed unless the information is unexpected. Notifications about interesting system-level conditions which are not error conditions. Informational in nature but having a more important need-to-know status. Examples are:

- System-wide notifications
- Process is shutting down gracefully on request
- Clearing of previously raised conditions
- A device or subsystem un-registering or shutting down for expected and normal reason (for individual phone related expected and normal unregistering or shutting down, informational level should be used)
- Password change notification and upgrade notification

authExpired

Authentication failure due to expired soft lock. User credentials have expired.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.
8.0(1)	Added Routing List element and updated the parameter list.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Notice (5)

Routing List

Event Log

Parameters

Authentication failure due to expired soft lock.(String)

Recommended Action

Administrator may reset the credential.

authMustChange

Authentication failed because it is marked that it must be changed by the user.“User must change” is set on this credential. The user must change the credential.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.
8.0(1)	Added more description and Routing List element. Corrected the parameter.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Notice (5)

Routing List

Event Log

Parameters

UserID[String]

Recommended Action

User or Administrator may reset credential.

BChannelISV

B-channel is in service.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Changed severity level from Informational to Notice.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Parameters

Channel Id. [UInt] Unique channel ID [String] Device name. [String]

Recommended Action

None

CallManagerOnline

Cisco CallManager service has completed initialization is online.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice (5)

Parameters

CCM Version [String]

Recommended Action

None

CertValidityOver30Days

Alarm indicates that the certificate expiry is approaching but the expiry date is more than 30 days.

Cisco Unified Serviceability Alarm Definition Catalog

System/CertMonitorAlarmCatalog

Severity

Notice(5)

Routing List

Event Log

Sys Log

Parameters

Message(String)

Recommended Action

Regenerate the certificate that is about to expire by accessing the Cisco Unified Operating System and go to Certificate Management. If the certificate is issued by a CA, generate a CSR, submit the CSR to CA, obtain a fresh certificate from CA, and upload it to Cisco Unified CM.

CodeYellowExit

CodeYellowExit. Unified CM has ceased throttling calls and has exited the Code Yellow state.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Notice.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Parameters

Expected Average Delay [UInt] Entry Latency [UInt] Exit Latency [UInt] Sample Size [UInt] Time Spent in Code Yellow [UInt] Number of Calls Rejected Due to Call Throttling [UInt] Total Code Yellow Exit [UInt]

Recommended Action

None

credReadFailure

Error occurred attempting to read a credential in the database. This could be a network or database issue.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.
8.0(1)	Changed severity level to Notice from Informational.Corrected parameter and added Routing List element.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Notice (5)

Routing List

Event

Parameters

Credential read failure for(String)

Recommended Action

Ensure credential (user name) exists. Could be a database problem.

DbInsertValidatedDIDFailure

The Insertion of a IME provided e164DID has failed. A failure occurred attempting to insert a Cisco Unified Active Link learned DID

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

NOTICE

Routing List

SDL

SDI

Sys Log

Event Log

SNMP Traps

Data Collector

Parameter(s)

e164 DID(String)

Granting Domain(String)

Recommended Action

Verify the DID and the granting domain. Check other associated alarms. Verify the database integrity.

DChannelISV

Indicated D-channel has gone in service.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Informational to Notice.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Parameters

Channel Id. [UInt] Unique channel Id [String] Device Name. [String] Device IP address [String]

Recommended Action

None

EMAppStopped

EM Application started.Application is shutting down gracefully because of an unloaded from Tomcat.

Cisco Unified Serviceability Alarm Definition Catalog

System/EMAlarmCatalog

Severity

NOTICE

Routing List

Sys Log

Event Log

Parameter(s)

Servlet Name(String)

Recommended Action

No action required.

EndPointRegistered

This alarm occurs when a device is successfully registered with Cisco Unified Communications Manager.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

NOTICE

Routing List

SDL

SDI

Sys Log

Data Collector

SNMP Traps

Alternate Syslog

Parameter(s)

Device name(String)

Device MAC address(String)

Device IP address(String)

Protocol(String)

Device description(String)

User ID(String)

Load ID(String)

Associated directory numbers(String)

Performance monitor object type(Enum)

Device type(Enum)

Configured Gatekeeper Name(String)

Technology Prefix Name(String)

Zone Information(String)

Alternate Gatekeeper List(String)

Active Gatekeeper(String)

Call Signal Address(String)

RAS Address(String)

IPV6Address(String)

IPAddressAttributes(Enum)

IPV6AddressAttributes(Enum)

ActiveLoadId(String)

InactiveLoadId(String)

Recommended Action

No action is required.

Related Topics

Performance Monitor Object Type Enum Definitions for EndPointRegistered, on page 353
Device Type Enum Definitions for EndPointRegistered, on page 353
IPAddressAttributes Enum Definitions for EndPointRegistered, on page 356
IPV6AddressAttributes Enum Definitions for EndPointRegistere, on page 356

Performance Monitor Object Type Enum Definitions for EndPointRegistered

Value	Definition
2	Cisco Phone

Device Type Enum Definitions for EndPointRegistered

Value	Definition
1	CISCO_30SP+
2	CISCO_12SP+
3	CISCO_12SP
4	CISCO_12S
5	CISCO_30VIP
6	CISCO_7910
7	CISCO_7960
8	CISCO_7940

Value	Definition
9	CISCO_7935
12	CISCO_ATA_186
20	SCCP_PHONE
61	H323_PHONE
72	CTI_PORT
115	CISCO_7941
119	CISCO_7971
255	UNKNOWN
302	CISCO_7989
307	CISCO_7911
308	CISCO_7941G_GE
309	CISCO_7961G_GE
335	MOTOROLA_CN622
336	BASIC_3RD_PARTY_SIP_DEVICE
348	CISCO_7931
358	CISCO_UNIFIED_COMMUNICATOR
365	CISCO_7921
369	CISCO_7906
374	ADVANCED_3RD_PARTY_SIP_DEVICE
375	CISCO_TELEPRESENCE
404	CISCO_7962
412	CISCO_3951
431	CISCO_7937
434	CISCO_7942

Value	Definition
435	CISCO_7945
436	CISCO_7965
437	CISCO_7975
446	CISCO_3911
468	CISCO_UNIFIED_MOBILE_COMMUNICATOR
478	CISCO_TELEPRESENCE_1000
479	CISCO_TELEPRESENCE_3000
480	CISCO_TELEPRESENCE_3200
481	CISCO_TELEPRESENCE_500
484	CISCO_7925
493	CISCO_9971
495	CISCO_6921
496	CISCO_6941
497	CISCO_6961
20000	CISCO_7905
30002	CISCO_7920
30006	CISCO_7970
30007	CISCO_7912
30008	CISCO_7902
30016	CISCO_IP_COMMUNICATOR
30018	CISCO_7961
30019	CISCO_7936
30035	IP_STE

IPAddressAttributes Enum Definitions for EndPointRegistered

Value	Definition
0	Unknown - The device has not indicated what this IPv4 address is used for
1	Administrative only - The device has indicated that this IPv4 address is used for administrative communication (web interface) only
2	Signal only - The device has indicated that this IPv4 address is used for control signaling only
3	Administrative and signal - The device has indicated that this IPv4 address is used for administrative communication (web interface) and control signaling

IPV6AddressAttributes Enum Definitions for EndPointRegistere

Value	Definition
0	Unknown - The device has not indicated what this IPv6 address is used for
1	Administrative only - The device has indicated that this IPv6 address is used for administrative communication (web interface) only
2	Signal only - The device has indicated that this IPv6 address is used for control signaling only
3	Administrative and signal - The device has indicated that this IPv6 address is used for administrative communication (web interface) and control signaling

H323Started

Cisco CallManager is ready to handle calls for the indicated H323 device. Cisco Unified Communications Manager is ready to communicate with the indicated H.323 device. Note that this alarm describes the readiness of Unified CM to communicate with the indicated device, but does not provide information about the state of the H.323 device (whether it is ready to communicate as well).

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Informational to Notice. • Following information updated: ◦ Parameters ◦ Enum Definitions for DeviceType

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Parameters

Device Name. [String] IP Address [String] Device type. [Optional] [Enum]Device description [Optional]. [String] The Server 1 IP Address/Host Name as configured in the Trunk Configuration window [String] Remote CallManager Server 2[Optional]. [String] Remote CallManager Server 3[Optional]. [String]

Recommended Action

None

Related Topics

DeviceType Enum Definitions for H323Started, on page 357

DeviceType Enum Definitions for H323Started

Code	Device Type
61	H323_PHONE
62	H323_GATEWAY
122	GATEKEEPER
125	TRUNK

ICTCallThrottlingEnd

Cisco CallManager starts handling calls for the indicated H323 device. Cisco CallManager has ceased throttling calls on the indicated H.323 device.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Error to Notice.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Parameters

Device Name. [String] IP Address [String] Device type. [Optional] [Enum]Device description [Optional]. [String]

Enum Definitions for DeviceType

- 125—TRUNK

Recommended Action

None.

kDeviceMgrMoreThan50SocketEvents

More than 50 events returned from TCP link. The specified Cisco Unified Communications Manager TCP link has returned a large number of TCP events. This indicates an unexpected flood of events.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.

Cisco Unified CommunicationsRelease	Action
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Severity changed from Informational to Notice.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Notice

Parameters

Trace Name [String]

Recommended Action

No action is required. Monitor for reoccurrence. This could be an indication of a security issue.

MGCPGatewayGainedComm

The MGCP gateway has established communication with Cisco Unified Communications Manager.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Informational to Notice.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Parameters

Device Name [String]

Recommended Action

Informational purposes only; no action is required.

MaxCallDurationTimeout

An active call was cleared because the amount of time specified in the Maximum Call Duration Timer service parameter had elapsed. If the allowed call duration is too short, you can increase the value. If you do not want a limit on the duration of an active call, you can disable the limit. If the duration is correct but you did not expect a call to ever exceed that duration, check the trace information around the time that this alarm occurred to try to determine if a gateway port had failed to release a call.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Informational to Notice. • Following parameters added: ◦ Originating Device name(String) ◦ Destination Device name(String) ◦ Call start time(UInt) ◦ Call stop time(UInt) ◦ Calling Party Number(String) ◦ Called Party Number(String)

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Parameters

Maximum Call Duration (minutes) [UInt]

Originating Device name(String)

Destination Device name(String)

Call start time(UInt)

Call stop time(UInt)

Calling Party Number(String)

Called Party Number(String)

Recommended Action

If the duration of the call is too short, increase the value in the Cisco CallManager service parameter or disable the maximum duration by setting the Maximum Call Duration Timer parameter to zero. If you suspect a hung gateway port, check the trace files around the time that this alarm occurred to search for the gateway that was involved in the call, then check the status of that gateway to determine if all ports are functioning normally.

SDLLinkISV

SDL link to remote application is restored. This alarm indicates that the local Cisco CallManager has gained communication with the remote Cisco CallManager.

Note The remote Cisco CallManager should also indicate SDLLinkISV with a different LinkID.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Informational to Notice.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Parameters

Remote IP address of remote application [String] Unique Link ID. [String] Local node ID [UInt] Local Application ID. [Enum]RemoteNodeID [UInt] Remote application ID. [Enum]

Recommended Action

None

Related Topics

LocalApplicationId and RemoteApplicationID Enum Definitions SDLLinkISV, on page 362

LocalApplicationId and RemoteApplicationID Enum Definitions SDLLinkISV

Code	Reason
100	CallManager
200	CTI Manager

SIPNormalizationScriptOpened

Cisco Unified CM opened the script for the SIP device.

The normalization script for the indicated SIP device has been successfully loaded, initialized, and activated on Cisco Unified CM.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	• New alarm for this release.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

Device Name(String)

Script Name(String)

In Use Memory(UInt)

Recommended Action

Notification purposes only; no action is required.

SIPNormalizationScriptClosed

Cisco Unified CM has closed the script for the SIP device. The script is closed at one of the following conditions:

- The indicated device (SIP trunk) was reset manually or automatically.
- The trunk was deleted manually.
- Due to script error or resource error or internal error.

When the script is closed, Cisco Unified CM will not invoke normalization script message handlers for the indicated SIP device.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	• New alarm for this release.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

Device Name(String)

Script Name(String)

Reason Code(Enum)

Reason Text(String)

Additional Information(String)

Recommended Action

This alarm serves as a notification of the script closure, if the alarm has occurred due to a SIP trunk maintenance window or any other expected reason for the script to close. If this alarm is unexpected, check for an occurrence of the SIPNormalizationScriptError alarm and refer to the specific action based on the reason code identified in the SIPNormalizationScriptError alarm.

Related Topics

Reason Code Enum Definitions for SIPNormalizationScriptClosed, on page 364

Reason Code Enum Definitions for SIPNormalizationScriptClosed

Value	Definition
1	DeviceResetManually—The associated device is reset manually using Cisco Unified CM Administration.
2	DeviceResetAutomatically—The associated device is reset automatically; the reset was triggered by an execution error in the script.
3	DeviceDeleted—The associated device is manually deleted in Cisco Unified CM Administration.
4	ScriptDisassociated—A configuration change occurred in Cisco Unified CM Administration and the script is no longer associated with the device.
5	ScriptInfoChanged—A change in the script logic occurred or a change to one or more fields on the SIP Normalization Script Configuration window in Cisco Unified CM Administration occurred.
6	ScriptError—An error occurred in the script; check for the occurrence of SIPNormalizationScriptError alarm and perform the recommended actions described to correct the script error.

SIPNormalizationAutoResetDisabled

An error occurred repeatedly and Cisco Unified CM disabled the script.

The script failed due to execution errors that occurred three times within a 10 minute period. As a result, the normalization script for the indicated SIP device has been disabled. Cisco Unified CM do not attempts to automatically reset either the script or the device for the purpose of recovering the script.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	• New alarm for this release.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

Device Name(String)

Script Name(String)

Script Type(String)

Reason Code(Enum)

Reason Text(String)

Additional Information(String)

Recommended Action

Notification purposes; examine the information and perform the recommended actions in the SIPNormalizationScriptError alarm, which should have been issued before this alarm.

Related Topics

Reason Code Enum Definitions for SIPNormalizationAutoResetDisabled, on page 366

Reason Code Enum Definitions for SIPNormalizationAutoResetDisabled

Value	Definition
1	ScriptResetDisabled—The system has automatically reset the script three times within a 10 minute period due to script execution errors; on the fourth occurrence of this error, Cisco Unified CM disabled the script.
2	TrunkResetDisabled—The system has automatically reset the trunk three times within a 10 minute period due to script execution errors; on the fourth occurrence of this error, Cisco Unified CM disabled the script.

SIPStarted

Cisco CallManager is ready to handle calls for the indicated SIP device. This alarm does not indicate the current state of the SIP device, only that Cisco CallManager is prepared to handle calls to or from the SIP device.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Severity changed from Informational to Notice. • Enum Definitions for InTransportType and OutTransportType are updated.
7.1	IPV6Address parameter added.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Parameters

Device Name. [String]

IP Address [Optional]. [String]

Device type. [Optional] [Enum]

Device description [Optional]. [String]

Incoming Port Number. [UInt]

Outgoing Port Number. [UInt]

Incoming Transport Type [Enum]

Outgoing Transport Type [Enum]

IPV6Address [Optional]. [String]

Recommended Action

None

Related Topics

DeviceType Enum Definitions for SIPStarted, on page 367
InTransportType Enum Definitions for SIPStarted, on page 367
OutTransportType Enum Definitions for SIPStarted, on page 367

DeviceType Enum Definitions for SIPStarted

- 131—SIP_TRUNK

InTransportType Enum Definitions for SIPStarted

Code	Definition
1	TCP
2	UDP
3	TLS
4	TCP/UDP

OutTransportType Enum Definitions for SIPStarted

Code	Definition
1	TCP
2	UDP

Code	Definition
3	TLS

SIPTrunkISV

All remote peers are available to handle calls for this SIP trunk.

This alarm indicates that all the remote peers are available to handle the calls for this SIP trunk. For each peer, the alarm provides the resolved IP address and port number, and hostname or SRV (if configured on SIP trunk).

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	New alarm for this release.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Notice

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

SIP Trunk Name(String)

Available remote peers for this SIP trunk(String)

Recommended Action

Notification purpose only; no action is required.

TestAlarmNotice

Testing notice alarm.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Test

Severity

Notice (5)

Recommended Action

None

TotalProcessesAndThreadsExceededThresholdEnd

The current total number of processes and threads is less than the maximum number of tasks configured in the Cisco RIS Data Collector service parameter, Maximum Number of Processes and Threads.

This can occur because a product which was integrated into Cisco Unified Communications Manager has been disabled or deactivated, which reduces the total number of processes and threads running on the system. Another cause for the number of processes or thread to decrease is that one or more processes has been stopped, which reduces the total number of processes and threads running on the system.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Informational to Notice.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/System Access

Severity

Notice

Parameters

NumberOfProcesses [String] NumberOfThreads [String] Reason [String]

Recommended Action

This alarm is for information purposes only; no action is required.

Informational-Level Alarms

The informational-level of alarm is 6 and no action is needed. Informational messages provide historical data such as internal flows of the application or per-request information. Informational messages are used for troubleshooting by users who are familiar with the basic flows of the application. An example would be a normal (expected) event occurred that the customer may want to be notified about.

AdministrativeEvent

Failed to write into the primary file path. Audit Event is generated by this application.

Cisco Unified Serviceability Alarm Catalog

AuditLog

Severity

INFORMATIONAL

Recommended Action

Ensure that the primary file path is valid and the corresponding drive has sufficient disk space. Also, make sure that the path has security permissions similar to default log file path.

AdminPassword

Administrative password got changed. If the change was unsuccessful or successful, a message gets displayed.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.
8.0(1)	Added descriptive text.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Informational (6)

Parameters

(String)

Recommended Action

None

AuditEventGenerated

Audit Event is generated by this application because failed to write into the primary file path.

Cisco Unified Serviceability Alarm Definition Catalog

System/Generic

Severity

Informational (6)

Parameters

UserID (String)

ClientAddress (String)

EventType (String)

ResourceAccessed(String)

EventStatus (String)

AuditDetails (String)

ComponentID (String)

Recommended Action

Ensure that the primary file path is valid and the corresponding drive has sufficient disk space. Also, make sure that the path has security permissions similar to default log file path.

AgentOnline

Agent online

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Informational (6)

Recommended Action

None

AgentOffline

Agent offline

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Informational (6)

Recommended Action

None

AuthenticationSucceeded

Login Authentication succeeded.

Facility/Sub-Facility

CCM_TOMCAT_APPS-LOGIN

Cisco Unified Serviceability Alarm Definition Catalog

System/Login

Severity

Informational (6)

Parameters

Login IP Address/Hostname [String] Login Date/Time [String] Login UserID [String] Login Interface [String]

Recommended Action

If this event is expected, no action is required; otherwise, notify the administrator.

authSuccess

Successfully authenticated this user.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.
8.5(1)	Parameter updated.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Informational (6)

Parameters

UserID(String)

Recommended Action

None

BDIStarted

Application started successfully.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Recommended Action

None

BuildStat

Device configuration files are being built. This alarm provides information about the BUILD ALL operation to build all types of configuration files.

Facility/Sub-Facility

CCM_TFTP-TFTP

Cisco Unified Serviceability Alarm Definition Catalog

System/TFTP

Severity

Informational (6)

Parameters

DeviceCount [Int] DeviceTime [Int] UnitCount [Int] UnitTime [Int] SoftkeyCount [Int] SoftkeyTime [Int] DialruleCount [Int] DialruleTime [Int] TotalTime [Int] BuildStatus [String]

Recommended Action

This alarm is for information purposes only; no action is required.

CiscoDirSyncStarted

Cisco DirSync Application started. Application started successfully.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Recommended Action

None

CiscoDirSyncProcessStarted

LDAPSync process started to sync user data on configured agreement ID.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

AgreementId [String]

Recommended Action

None

CiscoDirSyncProcessCompleted

LDAPSync process completed on particular sync agreement.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

AgreementId [String]

Recommended Action

None

CiscoDirSyncProcessStoppedManually

LDAPSync process stopped manually on particular sync agreement.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

AgreementId [String]

Recommended Action

None

CiscoDirSyncProcessStoppedAuto

LDAPSync process stopped automatically on particular sync agreement. It will restart automatically.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

AgreementId [String]

Recommended Action

None

CLM_ConnectivityTest

CLM Connectivity Test Failed. Cluster Manager detected a network error.

Facility/Sub-Facility

CCM_CLUSTERMANAGER/CLUSTERMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Cluster Manager

Severity

Informational (6)

Operating System

Appliance

Parameters

Node's IP(String)

Error (String)

Recommended Action

Verify connectivity between cluster nodes.

CLM_IPSecCertUpdated

IPSec self-signed cert updated. The IPSec self-signed cert from a peer node in the cluster has been imported due to a change.

Facility/Sub-Facility

CCM_CLUSTERMANAGER/CLUSTERMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Cluster Manager

Severity

Informational (6)

Operating System

Appliance

Parameters

Node's or IP(String)

Recommended Action

None

CLM_IPAddressChange

IP address change in cluster. The IP address of a peer node in the cluster has changed.

Facility/Sub-Facility

CCM_CLUSTERMANAGER/CLUSTERMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Cluster Manager

Severity

Informational (6)

Operating System

Appliance

Parameters

Node's (String)

Node's Old IP(String)

Node's New IP(String)

Recommended Action

None

CLM_PeerState

Current ClusterMgr session state.The ClusterMgr session state with another node in the cluster has changed to the current state.

Facility/Sub-Facility

CCM_CLUSTERMANAGER/CLUSTERMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Cluster Manager

Severity

Informational (6)

Operating System

Appliance

Parameters

Node's or IP(String)

Node's State(String)

Recommended Action

None

credFullUpdateSuccess

Credential was successfully updated.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Informational (6)

Parameters

(String)

Recommended Action

None

credFullUpdateFailure

An error was encountered during update of credential fields.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Informational (6)

Parameters

(String)

Recommended Action

Determine the issue and retry.

credReadSuccess

Successfully read a credential.

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Informational (6)

Parameters

(String)

Recommended Action

None

credUpdateFailure

The credential update failed most likely because the credential did not pass the security requirements (too short or credential used before, for example).

History

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.
8.0(1)	Added more descriptive text.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Informational (6)

Parameters

Credential Update Failure for(String)

Recommended Action

Determine issue (check length requirements, etc.) for this credential and retry.

credUpdateSuccess

Credential was successfully updated.

Cisco Unified CommunicationsRelease	Action
7.0(1)	Error message added.

Cisco Unified Serviceability Alarm Definition Catalog

System/IMS

Severity

Informational (6)

Parameters

Credential Update success for(String)

Recommended Action

None

DirSyncScheduledTaskOver

Directory synchronization operation started.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

SchedulerID [String] TaskID [String]

Recommended Action

None

DirSyncSchedulerEngineStopped

DirSync scheduler engine stopped.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

DirSyncSchedulerVersion [String]

Recommended Action

None

DirSyncNewScheduleInserted

New schedule inserted in the DirSync Scheduler.

Facility/Sub-Facility

CCM_JAVA_APPS/JAVAAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

EngineScheduleID [String]

Recommended Action

None

DRFLA2MAFailure

DRF Local Agent to Master Agent connection has some problems.

History

Cisco Unified Communications ManagerRelease	Action
8.0(1)	New name changed from CiscoDRFLA2MAFailure.

Facility/Sub-Facility

CCM_JAVA_APPS/JAVAAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Informational (6)

Parameters

Reason [String]

Recommended Action

Check if the Master Agent is up and the port is authorized.

DRFMA2LAFailure

Master Agent was unable to send a backup/restore request to the local agent.

History

Cisco Unified Communications ManagerRelease	Action
8.0(1)	New name changed from CiscoDRFMA2LAFailure. Descriptive text and Recommended action changed.

Facility/Sub-Facility

CCM_JAVA_APPS/JAVAAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Informational (6)

Parameters

Reason [String]

Recommended Action

Restart the corresponding local agents and the master agent.

CiscoDRFComponentRegistered

DRF Successfully Registered the requested component.

History

Cisco Unified Communications ManagerRelease	Action
8.0(1)	Name changed from CiscoDRFComponentRegistered.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Informational (6)

Parameters

Reason(String)

Recommended Action

Ensure that the registered component is needed for backup/restore operation.

CiscoDhcpdRestarted

DHCP Daemon restarted successfully.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

Reason [String]

Recommended Action

None

CiscoHardwareLicenseInvalid

Installation on invalid or obsolete hardware. Cannot upload license files.

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

INFORMATIONAL

Routing List

Sys Log

Event Log

SNMP Traps

Parameter(s)

Reason(String)

Recommended Action

Obtain correct hardware and reinstall.

CiscoLicenseFileInvalid

License File is invalid.

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

INFORMATIONAL

Routing List

Sys Log

Event Log

SNMP Traps

Parameter(s)

Reason(String)

Recommended Action

Rehost the License files.

CMInitializationStateTime

Indicates the amount of time required to complete initialization for the specified state.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational (6)

Parameters

Initialization State [String] Initialization Time [String] Initialization Time in Milliseconds [UInt]

Recommended Action

None

CMIServiceStatus

CMI service is running and working properly.Cisco Unified Serviceability Alarm Definition Catalog.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCMIServiceStatus.

Cisco Unified Serviceability Alarm Definition Catalog

CMIAlarmCatalog/CMI

Severity

INFORMATIONAL

Routing List

Event Log

SDI

Parameter(s)

Service Priority(String)

Recommended Action

Informational purpose only; no action is required.

CMTotalInitializationStateTime

Indicates the amount of time required to complete the specified total system initialization state.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational (6)

Parameters

Total Initialization Time [String] Total Initialization Time in Milliseconds [UInt]

Recommended Action

None

ConnectionToPDPInService

A connection was successfully established between Cisco Unified Communications Manager (Unified CM) and the policy decision point (PDP).

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational(6)

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

Policy Decision Point(String)

Recommended Action

None

CriticalEvent

Failed to write into the primary file path. Audit Event is generated by this application.

Cisco Unified Serviceability Alarm Catalog

AuditLog

Severity

INFORMATIONAL

Recommended Action

Ensure that the primary file path is valid and the corresponding drive has sufficient disk space. Also, make sure that the path has security permissions similar to default log file path.

CtiDeviceClosed

Application closed a device.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiDeviceClosed.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameter(s)

Device Name(String)

RTP Address(String)

Reason code.(Enum)

Recommended Action

This alarm is for informational purposes only; no action is required.

Related Topics

Reason Code Enum Definitions for CtiDeviceClosed, on page 389

Reason Code Enum Definitions for CtiDeviceClosed

Value	Definition
0	Unknown

Value	Definition
1	CallManager service is not available to process request; verify that the CallManager service is active. Check the Cisco Unified Serviceability Control Center section in Cisco Unified CM Administration (**Tools** > **Control Center - Feature Services**)
2	Device has unregistered with Cisco Unified Communications Manager
3	Device failed to rehome to Cisco Unified Communications Manager; verify that the device is registered
4	Device is removed from the Unified CM database
5	Application controlling the device has closed the connection
6	Route Point already registered by another application
7	CTI Port already registered by another application
8	CTI Port/Route Point already registered with dynamic port media termination
9	Enabling softkey failed for device; verify that the device is registered
10	Multiple applications have registered the device with media capability that do not match
11	This device is already controlled by another application
12	Protocol used by the device is not supported
13	Device is restricted for control by any application
14	Unable to communicate with database to retrieve device information
15	Device is resetting
16	Unable to register the device as specified media type is not supported
17	Unsupported device configuration
18	Device is being reset
19	IPAddress mode does not match what is configured in Unified CM

CtiDeviceInService

Device is back in service.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiDeviceInService.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Device Name(String)

Recommended Action

This alarm is for informational purposes only; no action is required.

CtiDeviceOpened

Application opened a device.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiDeviceOpened.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameter(s)

Device Name(String)

RTP Address(String)

Recommended Action

This alarm is for informational purposes only; no action is required.

CtiLineOpened

Application opened the line.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiLineOpened.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameter(s)

Directory Number(String)

Partition(String)

Device Name(String)

Recommended Action

This alarm is for informational purposes only; no action is required.

CtiLineOutOfService

Line is out of service.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiLineOutOfService.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Directory Number(String)

Device Name(String)

Recommended Action

This alarm is for informational purposes only; no action is required.

CtiProviderClosed

CTI application closed the provider. The IP address is shown in either IPv4 or IPv6 format depending on the IP addressing mode of the application.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiProviderClosed.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameter(s)

Login User Id(String)

IPAddress(String)

IPV6Address(String)

Reason code(Enum)

Recommended Action

This alarm is for informational purposes only; no action is required.

Related Topics

Reason Code Enum Definitions for CtiProviderClosed, on page 394

Reason Code Enum Definitions for CtiProviderClosed

Value	Definition
0	Unknown

Value	Definition
1	Heart beat from application missed. Possible causes include network connectivity issues or Unified CM node experiencing high CPU usage. Make sure that the network connectivity between Unified CM and the application by pinging the application server host from Cisco Unified OS Administration and take steps to establish connectivity if it has been lost. Also check for and fix any network issues or high CPU usage on the application server
2	Unexpected shutdown; possibly cause is application disconnected the TCP connection. Also check for and fix any network issues or high CPU usage on the application server
3	Application requested provider close
4	Provider open failure; application could not be initialized
5	User deleted. User associated with the application is deleted from the Unified CM Administration
6	SuperProvider permission associated with the application is removed. Verify the user group configuration for the user in Unified CM Admin under (**User Management** > **End User/Application User**), select the user and review the associated permissions information
7	Duplicate certificate used by application. Verify the CAPF profile configuration for the user in Unified CM Admin under (**User Management** > **End User CAPF Profile/Application User CAPF Profile**), select the CAPF profile of the user and review the associated information
8	CAPF information unavailable. Verify the CAPF profile configuration for the user in Unified CM Admin under (User **User Management** > **End User CAPF Profile/Application User CAPF Profile**), select the CAPF profile of the user and review the associated information
9	Certificate compromised. Verify the CAPF profile configuration for the user in Unified CM Admin under (**User Management** > **End User CAPF Profile/Application User CAPF Profile**), select the CAPF profile of the user and review the associated information
11	User is not authorized to connect to CTI using TLS. Consider the application configuration and security configuration for the user, for TAPI applications review the **Control Panel** > **Phone and Modem Options** > **Advanced** > **select a CiscoTSP** > **Configure...** > **Security** and disable “Secure Connection to CTIManager”. For JTAPI applications from JTPrefs choose Security and disable “Enable Secure Connection”. Also check the user group configuration for the user in Unified CM Admin under (**User Management** > **End User/Application User**), select the user and verify the associated permissions information

Value	Definition
12	Standard CTI Use permission removed. Users associated with applications are required to be included in “Standard CTI Enabled” user group. Verify the user group configuration for the user in Unified CM Admin under (**User Management** > **End User/Application User**), select the user and review the associated permissions information

CtiProviderOpened

CTI Application opened the provider successfully. The IP address is shown in either IPv4 or IPv6 format depending on the IP addressing mode of the Application.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiProviderOpened.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameter(s)

Login User Id(String)

Version Number(String)

IPAddress(String)

IPV6Address(String)

Recommended Action

This alarm is for informational purposes only; no action is required.

CtiDeviceOutofService

Device is out of service.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiDeviceOutofService. Severity changed from Notice to Informational.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Device Name(String)

Recommended Action

This alarm is for informational purposes only; no action is required.

CtiLineClosed

Application closed the line.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiLineClosed. Severity changed from Notice to Informational.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

Parameter(s)

Directory Number(String)

Partition(String)

Device Name(String)

Reason code.(Enum)

Recommended Action

This alarm is for informational purposes only; no action is required.

Related Topics

Reason Code Enum Definitions for CtiLineClosed, on page 398

Reason Code Enum Definitions for CtiLineClosed

Value	Definition
0	Unknown
1	CallManager failure
2	Device has unregistered with Cisco Unified Communications Manager; wait for the device to register
3	CTI failed to rehome the line; verify that the device is registered
4	Undefined line, possible cause could be that line is no more active on that device due to extension mobility login or logout
5	Device removed
6	Provider controlling the device is closed

Value	Definition
7	Protocol used by the device is not supported
8	Application cannot control this line as CTI Allow Control is not enabled. Administrator has restricted the Line to be controllable by application. If the intent of the Administrator is to allow control of this line, enable the check box labelled Allow control of Device from CTI, in Unified CM Administration under **Call Routing** > **Directory Number** and choose the line that should be controlled by this application
9	Unable to register the device; application specified media type is not supported
10	Device is being reset; verify that the device is registered before opening the line
11	Unsupported device configuration

CtiLineInService

Line is back in service

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Name changed from kCtiLineInService. Severity changed from Notice to Informational.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Event Log

Recommended Action

This alarm is for informational purposes only; no action is required.

DatabaseDefaultsRead

Database default information was read successfully.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Notice to Informational.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational

Parameters

None

Recommended Action

None

DefaultDurationInCacheModified

Default value of a Certificate duration in cache is modified in the Service Parameter page. This usually means that the Default Certificate duration in cache value is modified in the Service Parameter page.

Cisco Unified Serviceability Alarm Catalog

System/TVS

Severity

INFORMATIONAL

Routing List

SDI

Event Log

Data Collector

Sys Log

Recommended Action

None

DeviceApplyConfigInitiated

Device Apply Config initiated.

This alarm occurs when a system administrator presses the Apply Config button in Cisco Unified Communications Manager (Unified CM). The Apply Config button initiates a conditional restart on devices that support conditional restart. This button triggers the system to determine if any relevant configuration has changed for the device. If the configuration changes can be applied dynamically, they are made without service interruption. If a change requires that the device reregister with Unified CM, reregistration occurs automatically. If a change requires a restart, the device will be automatically restarted. If the load ID for a device changes, the device will initiate a background download of the new firmware. The new firmware can then be applied immediately or at a later time. For phones and devices that do not support conditional restart, clicking Apply Config causes these devices to restart.

Severity

Informational

Routing List

SDL

SDI

Sys Log

Parameter(s)

Device name(String)

Product type(String)

Device type(Enum)

Enum Definitions for Device Type

- 493—CISCO_9971

Recommended Action

None

DeviceApplyConfigResult

Cisco IP Phone has applied its configuration.

History

Cisco Unified CommunicationsRelease	Action
7.1	Added DeviceApplyConfigResult to the Phone Catalog in the CallManager alarm definitions.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/Phone

Severity

Informational (6)

Parameters

DeviceName(String)

IPAddress(String)

UnifiedCM_Result(String)

Phone_Result(String)

Reason(String)

Recommended Action

No action is required.

DeviceDnInformation

List of directory numbers associated with the device.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational (6)

Parameters

Device Name [String] Device type. [Optional] [Enum]Station Desc [String] Station Dn [String]

Recommended Action

None

Related Topics

DeviceType Enum Definitions for DeviceDnInformation, on page 403

DeviceType Enum Definitions for DeviceDnInformation

Code	Device Type
1	CISCO_30SP+
2	CISCO_12SP+
3	CISCO_12SP
4	CISCO_12S
5	CISCO_30VIP
6	CISCO_7910
7	CISCO_7960
8	CISCO_7940
9	CISCO_7935
10	CISCO_VGC_PHONE
11	CISCO_VGC_VIRTUAL_PHONE
12	CISCO_ATA_186
20	SCCP_PHONE
21	STATION_PHONE_APPLICATION
30	ANALOG_ACCESS
40	DIGITAL_ACCESS
41	DIGITAL_ACCESS_T1
42	DIGITAL_ACCESS+
43	DIGITAL_ACCESS_WS-X6608
47	ANALOG_ACCESS_WS-X6624

Code	Device Type
48	VGC_GATEWAY
50	CONFERENCE_BRIDGE
51	CONFERENCE_BRIDGE_HARDWARE
52	CONFERENCE_BRIDGE_HARDWARE_HDV2
53	CONFERENCE_BRIDGE_HARDWARE_WS-SVC-CMM
61	H323_PHONE
62	H323_GATEWAY
70	MUSIC_ON_HOLD
71	DEVICE_PILOT
72	CTI_PORT
73	CTI_ROUTE_POINT
80	VOICE_MAIL_PORT
83	SOFTWARE_MEDIA_TERMINATION_POINT_HDV2
84	CISCO_MEDIA_SERVER
85	CISCO_VIDEO_CONFERENCE_BRIDGE
90	ROUTE_LIST
100	LOAD_SIMULATOR
110	MEDIA_TERMINATION_POINT
111	MEDIA_TERMINATION_POINT_HARDWARE
112	MEDIA_TERMINATION_POINT_HDV2
113	MEDIA_TERMINATION_POINT_WS-SVC-CMM
115	CISCO_7941
119	CISCO_7971
120	MGCP_STATION

Code	Device Type
121	MGCP_TRUNK
122	GATEKEEPER
124	7914_14_BUTTON_LINE_EXPANSION_MODULE
125	TRUNK
126	TONE_ANNOUNCEMENT_PLAYER
131	SIP_TRUNK
132	SIP_GATEWAY
133	WSM_TRUNK
134	REMOTE_DESTINATION_PROFILE
254	UNKNOWN_MGCP_GATEWAY
255	UNKNOWN
302	CISCO_7989
307	CISCO_7911
308	CISCO_7941G_GE
309	CISCO_7961G_GE
335	MOTOROLA_CN622
336	BASIC_3RD_PARTY_SIP_DEVICE
358	CISCO_UNIFIED_COMMUNICATOR
365	CISCO_7921
369	CISCO_7906
374	ADVANCED_3RD_PARTY_SIP_DEVICE
375	CISCO_TELEPRESENCE
404	CISCO_7962
412	CISCO_3951

Code	Device Type
431	CISCO_7937
434	CISCO_7942
435	CISCO_7945
436	CISCO_7965
437	CISCO_7975
20000	CISCO_7905
30002	CISCO_7920
30006	CISCO_7970
30007	CISCO_7912
30008	CISCO_7902
30016	CISCO_IP_COMMUNICATOR
30018	CISCO_7961
30019	CISCO_7936
30027	ANALOG_PHONE
30028	ISDN_BRI_PHONE
30032	SCCP_GATEWAY_VIRTUAL_PHONE
30035	IP_STE

DeviceImageDownloadStart

Cisco IP Phone has started downloading its firmware load (image).

History

Cisco Unified CommunicationsRelease	Action
7.1	Added DeviceImageDownloadStart to the Phone Catalog in the CallManager alarm definitions.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/Phone

Severity

Informational (6)

Routing List

SDL

SDI

Sys Log

Alternate Syslog

Data Collector

Parameters

DeviceName(String)

IPAddress(String)

Active(String)

RequestedLoadId(String

Recommended Action

No action is required.

DeviceImageDownloadSuccess

Cisco IP Phone has successfully downloaded its image.

History

Cisco Unified CommunicationsRelease	Action
8.1(5)	• Included Routing List. • Updated Parameters. • Included Enum Definitions - Method
7.1	Added DeviceImageDownloadSuccess to the Phone Catalog in the CallManager alarm definitions.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/Phone

Severity

Informational (6)

Routing List

SDL

SDI

Sys Log

Alternate Syslog

Data Collector

Parameters

DeviceName(String)

IPAddress(String)

Method(Enum)

Active(String)

Inactive(String)

Server from which the firmware was downloaded(String)

Recommended Action

No action is required.

Related Topics

Method Enum Definitions for DeviceImageDownloadSuccess, on page 408

Method Enum Definitions for DeviceImageDownloadSuccess

Value	Definition
1	TFTP
2	HTTP
3	PPID

DeviceRegistered

A device successfully registered with Cisco Unified Communications Manager.

History

Cisco Unified CommunicationsRelease	Action
8.5(1)	Following information is updated: • Enum Definitions for Performance Monitor ObjType
8.0(1)	Following information is updated: • Enum Definitions for Performance Monitor ObjType • Enum Definitions for Device type
7.1	Parameters added for IPv6: IPV6Address[Optional].[String], IPAddressAttributes[Optional].[Enum], IPV6AddressAttributes [Optional].[Enum], and ActiveLoadId [Optional].[String].

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational (6)

Routing List

SDL

SDI

Sys Log

Event Log

Data Collector

SNMP Traps

Parameters

Device name.[String]

Device MAC address [Optional].[String]

Device IP address [Optional].[String]

Protocol.[String]

Device description [Optional].[String]

User ID [Optional].[String]

Load ID. [Optional][String]

Associated directory numbers.[Optional].[String]

Performance monitor object type[Enum]

Device type. [Optional][Enum]

Configured GateKeeper Name [Optional].[String]

Technology Prefix Name [Optional].[String]

Zone Information [Optional].[String]

Alternate Gatekeeper List [Optional].[String]

Active Gatekeeper [Optional].[String]

Call Signal Address [Optional].[String]

RAS Address [Optional].[String]

IPV6Address[Optional].[String]

IPAddressAttributes[Optional].[Enum]

IPV6AddressAttributes [Optional].[Enum]

ActiveLoadId [Optional].[String]

InactiveLoadId [Optional].[String]

Recommended Action

None

Related Topics

Performance Monitor ObjType Enum Definitions for DeviceRegistered, on page 410
DeviceType Enum Definitions for DeviceRegistered, on page 412
IPAddrAttributes Enum Definitions for DeviceRegistered, on page 414
IPV6AddrAttributes Enum Definitions for DeviceRegistered, on page 414

Performance Monitor ObjType Enum Definitions for DeviceRegistered

Code	Reason
1	Cisco CallManager
3	Cisco Lines
4	Cisco H.323
5	Cisco MGCP Gateway
6	Cisco MOH Device
7	Cisco Analog Access
8	Cisco MGCP FXS Device

Code	Reason
9	Cisco MGCP FXO Device
10	Cisco MGCP T1CAS Device
11	Cisco MGCP PRI Device
12	Cisco MGCP BRI Device
13	Cisco MTP Device
14	Cisco Transcode Device
15	Cisco SW Conference Bridge Device
16	Cisco HW Conference Bridge Device
17	Cisco Locations
18	Cisco Gatekeeper
19	Cisco CallManager System Performance
20	Cisco Video Conference Bridge Device
21	Cisco Hunt Lists
22	Cisco SIP
23	Cisco Annunciator Device
24	Cisco QSIG Features
25	Cisco SIP Stack
26	Cisco Presence Features
27	Cisco WSMConnector
28	Cisco Dual-Mode Mobility
29	Cisco SIP Station
30	Cisco Mobility Manager
31	Cisco Signaling
32	Cisco Call Restriction

Code	Reason
33	External Call Control
34	Cisco SAF Client
35	IME Client
36	IME Client Instance

DeviceType Enum Definitions for DeviceRegistered

Code	Reason
10	CISCO_VGC_PHONE
11	CISCO_VGC_VIRTUAL_PHONE
30	ANALOG_ACCESS
40	DIGITAL_ACCESS
42	DIGITAL_ACCESS+
43	DIGITAL_ACCESS_WS-X6608
47	ANALOG_ACCESS_WS-X6624
48	VGC_GATEWAY
50	CONFERENCE_BRIDGE
51	CONFERENCE_BRIDGE_HARDWARE
52	CONFERENCE_BRIDGE_HARDWARE_HDV2
53	CONFERENCE_BRIDGE_HARDWARE_WS-SVC-CMM
62	H323_GATEWAY
70	MUSIC_ON_HOLD
71	DEVICE_PILOT
73	CTI_ROUTE_POINT
80	VOICE_MAIL_PORT

Code	Reason
83	SOFTWARE_MEDIA_TERMINATION_POINT_HDV2
84	CISCO_MEDIA_SERVER
85	CISCO_VIDEO_CONFERENCE_BRIDGE
90	ROUTE_LIST
100	LOAD_SIMULATOR
110	MEDIA_TERMINATION_POINT
111	MEDIA_TERMINATION_POINT_HARDWARE
112	MEDIA_TERMINATION_POINT_HDV2
113	MEDIA_TERMINATION_POINT_WS-SVC-CMM
120	MGCP_STATION
121	MGCP_TRUNK
122	GATEKEEPER
124	7914_14_BUTTON_LINE_EXPANSION_MODULE
125	TRUNK
126	TONE_ANNOUNCEMENT_PLAYER
131	SIP_TRUNK
132	SIP_GATEWAY
133	WSM_TRUNK
134	REMOTE_DESTINATION_PROFILE
227	7915_12_BUTTON_LINE_EXPANSION_MODULE
228	7915_24_BUTTON_LINE_EXPANSION_MODULE
229	7916_12_BUTTON_LINE_EXPANSION_MODULE
230	7916_24_BUTTON_LINE_EXPANSION_MODULE
232	CKEM_36_BUTTON_LINE_EXPANSION_MODULE

Code	Reason
254	UNKNOWN_MGCP_GATEWAY
255	UNKNOWN
30027	ANALOG_PHONE
30028	ISDN_BRI_PHONE
30032	SCCP_GATEWAY_VIRTUAL_PHONE

IPAddrAttributes Enum Definitions for DeviceRegistered

Code	Reason
0	Unknown—The device has not indicated what this IPv4 address is used for.
1	Administrative only—The device has indicated that this IPv4 address is used for administrative communication (web interface) only.
2	Signal only—The device has indicated that this IPv4 address is used for control signaling only.
3	Administrative and signal—The device has indicated that this IPv4 address is used for administrative communication (web interface) and control signaling.

IPV6AddrAttributes Enum Definitions for DeviceRegistered

Code	Reason
0	Unknown—The device has not indicated what this IPv6 address is used for.
1	Administrative only—The device has indicated that this IPv6 address is used for administrative communication (web interface) only.
2	Signal only—The device has indicated that this IPv6 address is used for control signaling only.
3	Administrative and signal—The device has indicated that this IPv6 address is used for administrative communication (web interface) and control signaling.

DeviceResetInitiated

Device reset initiated on the specified device.

This alarm occurs when a device is reset via the Reset button in Cisco Unified CM Administration. Reset may cause the device to shut down and come back in service. A device can be reset only when it is registered with Cisco Unified Communications Manager.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Enum Definitions for DeviceType are updated. • Parameters added: Product type [String]

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational (6)

Parameters

Device name [Optional]. [String] Device type. [Optional] [Enum] Product type [String]

Recommended Action

None

Related Topics

DeviceType Enum Definitions for DeviceResetInitiated, on page 415

DeviceType Enum Definitions for DeviceResetInitiated

Code	Device Type
10	CISCO_VGC_PHONE
11	CISCO_VGC_VIRTUAL_PHONE
30	ANALOG_ACCESS

Code	Device Type
40	DIGITAL_ACCESS
42	DIGITAL_ACCESS+
43	DIGITAL_ACCESS_WS-X6608
47	ANALOG_ACCESS_WS-X6624
48	VGC_GATEWAY
50	CONFERENCE_BRIDGE
51	CONFERENCE_BRIDGE_HARDWARE
52	CONFERENCE_BRIDGE_HARDWARE_HDV2
53	CONFERENCE_BRIDGE_HARDWARE_WS-SVC-CMM
62	H323_GATEWAY
70	MUSIC_ON_HOLD
71	DEVICE_PILOT
73	CTI_ROUTE_POINT
80	VOICE_MAIL_PORT
83	SOFTWARE_MEDIA_TERMINATION_POINT_HDV2
84	CISCO_MEDIA_SERVER
85	CISCO_VIDEO_CONFERENCE_BRIDGE
90	ROUTE_LIST
100	LOAD_SIMULATOR
110	MEDIA_TERMINATION_POINT
111	MEDIA_TERMINATION_POINT_HARDWARE
112	MEDIA_TERMINATION_POINT_HDV2
113	MEDIA_TERMINATION_POINT_WS-SVC-CMM
120	MGCP_STATION

Code	Device Type
121	MGCP_TRUNK
122	GATEKEEPER
124	7914_14_BUTTON_LINE_EXPANSION_MODULE
125	TRUNK
126	TONE_ANNOUNCEMENT_PLAYER
131	SIP_TRUNK
132	SIP_GATEWAY
133	WSM_TRUNK
134	REMOTE_DESTINATION_PROFILE
227	7915_12_BUTTON_LINE_EXPANSION_MODULE
228	7915_24_BUTTON_LINE_EXPANSION_MODULE
229	7916_12_BUTTON_LINE_EXPANSION_MODULE
230	7916_24_BUTTON_LINE_EXPANSION_MODULE
232	CKEM_36_BUTTON_LINE_EXPANSION_MODULE
254	UNKNOWN_MGCP_GATEWAY
255	UNKNOWN
30027	ANALOG_PHONE
30028	ISDN_BRI_PHONE
30032	SCCP_GATEWAY_VIRTUAL_PHONE

DeviceRestartInitiated

Device restart initiated or Apply Config initiated on the specified device.

This alarm occurs when a device is restarted via the Restart button in Cisco Unified CM Administration window or when a system administrator presses the Apply Config button for a device that does not support conditional restart. Restart causes the device to unregister, receive updated configuration, and reregister with Cisco Unified Communications Manager (Unified CM) without shutting down. A device can be restarted only when it is registered with Unified CM.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Enum Definitions for DeviceType are updated. • Parameters added: Product type [String]

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational (6)

Parameters

Device name [Optional]. [String] Device type. [Optional] [Enum] Product type [String]

Recommended Action

None

Related Topics

DeviceType Enum Definitions for DeviceRestartInitiated, on page 418

DeviceType Enum Definitions for DeviceRestartInitiated

Code	Device Type
10	CISCO_VGC_PHONE
11	CISCO_VGC_VIRTUAL_PHONE
30	ANALOG_ACCESS
40	DIGITAL_ACCESS
42	DIGITAL_ACCESS+
43	DIGITAL_ACCESS_WS-X6608
47	ANALOG_ACCESS_WS-X6624

Code	Device Type
48	VGC_GATEWAY
50	CONFERENCE_BRIDGE
51	CONFERENCE_BRIDGE_HARDWARE
52	CONFERENCE_BRIDGE_HARDWARE_HDV2
53	CONFERENCE_BRIDGE_HARDWARE_WS-SVC-CMM
62	H323_GATEWAY
70	MUSIC_ON_HOLD
71	DEVICE_PILOT
73	CTI_ROUTE_POINT
80	VOICE_MAIL_PORT
83	SOFTWARE_MEDIA_TERMINATION_POINT_HDV2
84	CISCO_MEDIA_SERVER
85	CISCO_VIDEO_CONFERENCE_BRIDGE
90	ROUTE_LIST
100	LOAD_SIMULATOR
110	MEDIA_TERMINATION_POINT
111	MEDIA_TERMINATION_POINT_HARDWARE
112	MEDIA_TERMINATION_POINT_HDV2
113	MEDIA_TERMINATION_POINT_WS-SVC-CMM
120	MGCP_STATION
121	MGCP_TRUNK
122	GATEKEEPER
124	7914_14_BUTTON_LINE_EXPANSION_MODULE
125	TRUNK

Code	Device Type
126	TONE_ANNOUNCEMENT_PLAYER
131	SIP_TRUNK
132	SIP_GATEWAY
133	WSM_TRUNK
134	REMOTE_DESTINATION_PROFILE
227	7915_12_BUTTON_LINE_EXPANSION_MODULE
228	7915_24_BUTTON_LINE_EXPANSION_MODULE
229	7916_12_BUTTON_LINE_EXPANSION_MODULE
230	7916_24_BUTTON_LINE_EXPANSION_MODULE
232	CKEM_36_BUTTON_LINE_EXPANSION_MODULE
254	UNKNOWN_MGCP_GATEWAY
255	UNKNOWN
30027	ANALOG_PHONE
30028	ISDN_BRI_PHONE
30032	SCCP_GATEWAY_VIRTUAL_PHONE

DirSyncScheduleInsertFailed

DirSync schedule insertion failed.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

ScheduleID [String]

Recommended Action

Check the DirSync configuration and logs

DirSyncSchedulerEngineStarted

DirSync scheduler engine started.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

DirSyncSchedulerVersion [String]

Recommended Action

None

DRFBackupCompleted

DRF backup completed successfully.

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

INFORMATIONAL

Routing List

Event Log

Sys Log

Parameter(s)

Reason(String)

Recommended Action

Ensure that the backup operation is completed successfully.

DRFRestoreCompleted

DRF restore completed successfully.

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

INFORMATIONAL

Routing List

Event Log

Sys Log

Parameter(s)

Reason(String)

Recommended Action

Ensure that the restore operation is completed successfully.

DRFSchedulerUpdated

DRF Scheduled backup configurations is updated automatically due to feature de-registration.

History

Cisco Unified Communications ManagerRelease	Action
8.0(1)	Name changed from CiscoDRFSchedulerUpdated.

Facility/Sub-Facility

CCM_DRF_LOCAL & CCM_DRF_MASTER/DRF

Cisco Unified Serviceability Alarm Definition Catalog

System/DRF

Severity

Informational (6)

Parameters

Reason(String)

Recommended Action

Ensure that the new configurations is appropriate one for the backup/restore operation.

EMAppStarted

EM Application started successfully.

Cisco Unified Serviceability Alarm Definition Catalog

System/EMAlarmCatalog

Severity

INFORMATIONAL

Routing List

Sys Log

Event Log

Parameter(s)

Servlet Name(String)

Recommended Action

No action required.

EMCCUserLoggedIn

EMCC login was successful.

Cisco Unified Serviceability Alarm Definition Catalog

System/EMAlarmCatalog

Severity

Informational(6)

Routing List

Sys Log

Event Log

Parameters

Device Name(String)

Login Date/Time(String)

Login UserID(String)

Recommended Action

None

EMCCUserLoggedOut

EMCC logout was successful.

Cisco Unified Serviceability Alarm Definition Catalog

System/EMAlarmCatalog

Severity

Informational(6)

Routing List

Sys Log

Event Log

Parameters

Device Name(String)

Login Date/Time(String)

UserID(String)

Recommended Action

None

EndPointResetInitiated

This alarm occurs when a device is reset via the Reset button in Cisco Unified CM Administration. Reset causes the device to shut down and come back in service. A device can be reset only when it is registered with Cisco Unified Communications Manager.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Alternate Syslog

Parameter(s)

Device name(String)

Product type(String)

Device type(Enum)

Recommended Action

Informational purposes only; no action is required.

Related Topics

Device Type Enum Definitions for EndPointResetInitiated, on page 425

Device Type Enum Definitions for EndPointResetInitiated

Value	Definition
1	CISCO_30SP+
2	CISCO_12SP+
3	CISCO_12SP
4	CISCO_12S
5	CISCO_30VIP
6	CISCO_7910
7	CISCO_7960
8	CISCO_7940
9	CISCO_7935
12	CISCO_ATA_186
20	SCCP_PHONE
61	H323_PHONE
72	CTI_PORT

Value	Definition
115	CISCO_7941
119	CISCO_7971
255	UNKNOWN
302	CISCO_7989
307	CISCO_7911
308	CISCO_7941G_GE
309	CISCO_7961G_GE
335	MOTOROLA_CN622
336	BASIC_3RD_PARTY_SIP_DEVICE
348	CISCO_7931
358	CISCO_UNIFIED_COMMUNICATOR
365	CISCO_7921
369	CISCO_7906
374	ADVANCED_3RD_PARTY_SIP_DEVICE
375	CISCO_TELEPRESENCE
404	CISCO_7962
412	CISCO_3951
431	CISCO_7937
434	CISCO_7942
435	CISCO_7945
436	CISCO_7965
437	CISCO_7975
446	CISCO_3911
468	CISCO_UNIFIED_MOBILE_COMMUNICATOR

Value	Definition
478	CISCO_TELEPRESENCE_1000
479	CISCO_TELEPRESENCE_3000
480	CISCO_TELEPRESENCE_3200
481	CISCO_TELEPRESENCE_500
484	CISCO_7925
493	CISCO_9971
495	CISCO_6921
496	CISCO_6941
497	CISCO_6961
20000	CISCO_7905
30002	CISCO_7920
30006	CISCO_7970
30007	CISCO_7912
30008	CISCO_7902
30016	CISCO_IP_COMMUNICATOR
30018	CISCO_7961
30019	CISCO_7936
30035 I	P_STE

EndPointRestartInitiated

Device restart initiated or Apply Config initiated on the specified device.

This alarm occurs when a device is restarted via the Restart button in Cisco Unified CM Administration window or when a system administrator presses the Apply Config button for a device that does not support conditional restart. Restart causes the device to unregister, receive an updated configuration file, and reregister with Cisco Unified Communications Manager (Unified CM) without shutting down. A device can be restarted only when it is registered with Unified CM.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Alternate Syslog

Parameter(s)

Device name(String)

Product type(String)

Device type(Enum)

Recommended Action

Informational purposes only; no action is required.

Related Topics

Device Type Enum Definitions for EndPointRestartInitiated, on page 428

Device Type Enum Definitions for EndPointRestartInitiated

Value	Definition
1	CISCO_30SP+
2	CISCO_12SP+
3	CISCO_12SP
4	CISCO_12S
5	CISCO_30VIP
6	CISCO_7910
7	CISCO_7960
8	CISCO_7940
9	CISCO_7935

Value	Definition
12	CISCO_ATA_186
20	SCCP_PHONE
61	H323_PHONE
72	CTI_PORT
115	CISCO_7941
119	CISCO_7971
255	UNKNOWN
302	CISCO_7989
307	CISCO_7911
308	CISCO_7941G_GE
309	CISCO_7961G_GE
335	MOTOROLA_CN622
336	BASIC_3RD_PARTY_SIP_DEVICE
348	CISCO_7931
358	CISCO_UNIFIED_COMMUNICATOR
365	CISCO_7921
369	CISCO_7906
374	ADVANCED_3RD_PARTY_SIP_DEVICE
375	CISCO_TELEPRESENCE
404	CISCO_7962
412	CISCO_3951
431	CISCO_7937
434	CISCO_7942
435	CISCO_7945

Value	Definition
436	CISCO_7965
437	CISCO_7975
446	CISCO_3911
468	CISCO_UNIFIED_MOBILE_COMMUNICATOR
478	CISCO_TELEPRESENCE_1000
479	CISCO_TELEPRESENCE_3000
480	CISCO_TELEPRESENCE_3200
481	CISCO_TELEPRESENCE_500
484	CISCO_7925
493	CISCO_9971
495	CISCO_6921
496	CISCO_6941
497	CISCO_6961
20000	CISCO_7905
30002	CISCO_7920
30006	CISCO_7970
30007	CISCO_7912
30008	CISCO_7902
30016	CISCO_IP_COMMUNICATOR
30018	CISCO_7961
30019	CISCO_7936
30035	IP_STE

EndThrottlingCallListBLFSubscriptions

CallManager has resumed accepting CallList BLF Subscriptions subsequent to prior throttling.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Severity changed from Warning to Informational.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational

Parameters

EndThrottlingCallListBLFSubscriptionsActive External Presence Subscriptions [UInt] CallList BLF Subscriptions Throttling Threshold [UInt] CallList BLF Subscriptions Resume Threshold [UInt] Time Duration Of Throttling CallList BLF Subscriptions [UInt] Number of CallList BLF Subscriptions Rejected Due To Throttling [UInt] Total End Throttling CallList BLF Subscriptions [UInt]

Recommended Action

Determine if CPU and memory resources are available to meet the higher demand for CallList BLF Subscriptions. If so, increase the CallListBLFSubscriptionsThrottlingThreshold and correspondingly the CallListBLFSubscriptionsResumeThreshold. If not, increase system resources to meet the demand.

IDSEngineDebug

Indicates debug events from IDS database engine. This alarm provides low-level debugging information from IDS database engine. System administrator can disregard this alarm.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Changed severity level to Informational from Debug.

Facility/Sub-Facility

CCM_DB_LAYER-DB

Cisco Unified Serviceability Alarm Definition Catalog

System/DB

Severity

Informational

Parameters

Event Class ID [String] Event class message [String] Event Specific Message [String]

Recommended Action

None

IDSEngineInformation

No error has occurred but some routine event completed in IDS database engine. This alarm is informational. No error has occurred but some routine event completed in IDS database engine.

Facility/Sub-Facility

CCM_DB_LAYER-DB

Cisco Unified Serviceability Alarm Definition Catalog

System/DB

Severity

Informational (6)

Parameters

Event Class ID [String] Event class message [String] Event Specific Message [String]

Recommended Action

None

IDSReplicationInformation

Information about IDS replication.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Added Recommended Action comments.

Facility/Sub-Facility

DB

Cisco Unified Serviceability Alarm Definition Catalog

System/DB

Severity

Informational (6)

Parameters

Event Class ID [String]

Event class message [String]

Event Specific Message [String]

Recommended Action

Information only. No action is required.

IPMAInformation

IPMA Information.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

Servlet Name [String] Reason [String]

Recommended Action

None

IPMAStarted

IPMA Application started successfully.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

Servlet Name [String] Reason [String]

Recommended Action

None

ITLFileRegenerated

New ITL File has been generated. This usually means that a new certificate related to ITLFile has been modified.

Cisco Unified Serviceability Alarm Catalog

System/TVS

Severity

INFORMATIONAL

Routing List

SDI

Event Log

Data Collector

Sys Log

Recommended Action

None.

kANNICMPErrorNotification

ANN stream ICMP port unreachable error. An announcement RTP stream had an ICMP (Internet Control Message Protocol) port unreachable error. The stream has been terminated. This ICMP error is a result of the destination end-point not having the receiving UDP/RTP port open to receive packets.

History

Cisco Unified CommunicationsRelease	Action
8.0.1	Parameter list updated.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational (6)

Parameters

Destination IP Address [String]

Recommended Action

No action is required. This may occur at times when connections are being stopped or redirected.

kCFBICMPErrorNotification

CFB stream ICMP error. A SW CFB RTP stream had an ICMP (Internet Control Message Protocol) port unreachable error. The stream has been terminated. This ICMP error is a result of the destination end-point does not have the receiving UDP/RTP port open to receive packets.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Following parameters removed: Call ID [ULong] Party ID [ULong] IP Port [ULong]

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational (6)

Parameters

Destination IP Address [String]

Recommended Action

No action is required. This may occur at times when connections are being stopped or redirected.

kReadCfgIpTosMediaResourceToCmNotFound

IP TOS MediaResource to Cm value not found. The IP Type-of-Service Media Resource To Call Manager service parameter value was not found in the database. Defaulting its value to 0x60 for CS3(precedence 3) DSCP (011000).

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1).

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational (6)

Recommended Action

Set the Ip Type-of-Service Media Resource To Call Manager service parameter for the Cisco IP Voice Media Streaming App service.

kDeviceMgrLockoutWithCallManager

Cisco Unified Communications Manager in lockout.The specified Cisco Unified Communications Manager has failed to respond to control messages. The TCP control connection to Cisco Unified CM is being suspended. This will cause a switch to another Cisco Unified CM if one is available otherwise the device will be unavailable. There may be a shortage of CPU resource or some other error condition on the Cisco Unified CM server.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Severity changed from Error to Informational.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational

Parameters

Trace Name [String]

Recommended Action

Check the status of the Cisco Unified Communications Manager service. You may have to restart the Cisco Unified CM service or the Cisco Unified CM server.

kDeviceMgrRegisterWithCallManager

Register with Cisco Unified Communications Manager. The software media device registered with the specified Cisco Unified Communications Manager.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1).

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational (6)

Parameters

Trace Name [String]

Recommended Action

None

kDeviceMgrThreadWaitFailed

Wait call failure in device manager thread. An error was reported during a system request to wait on an event, the media device will be restarted.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.

Cisco Unified CommunicationsRelease	Action
8.0(1)	This alarm is available in 8.0(1). • Severity changed from Error to Informational. • Following parameters added: ◦ OS Error Code [Int] ◦ OS Error Description [String]

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational

Parameters

Trace Name [String]

OS Error Code [Int]

OS Error Description [String]

Recommended Action

None

kDeviceMgrUnregisterWithCallManager

Unregister with Cisco Unified Communications Manager. A media device has unregistered with the specified Cisco Unified Communications Manager.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1).

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational (6)

Parameters

Trace Name [String]

Recommended Action

No action is required. The media device will automatically reregister.

kIPVMSStarting

The Cisco IP Voice Media Streaming App service is starting.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). ProcessID [ULong] parameter is removed.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational (6)

Parameters

Version [String] IPAddress [String] Hostname [String] ServiceName [String]

Recommended Action

No action is required.

kIPVMSStopping

The Cisco IP voice media streaming application is shutting down.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). ProcessID [ULong] parameter is removed.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational (6)

Parameters

Version [String] IPAddress [String] Hostname [String] ServiceName [String]

Recommended Action

No action is required.

kMOHICMPErrorNotification

MOH stream ICMP error. A Music-on-Hold transmission stream had an ICMP (Internet Control Message Protocol) port unreachable error. The stream has been terminated. This may occur occasionally depending on call termination sequences.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). Following parameters are removed: Call ID [ULong] Party ID [ULong] IP Port [ULong]

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational (6)

Parameters

Destination IP Address [String]

Recommended Action

No action is required.

kMOHMgrThreadWaitFailed

Wait call failure in MOH manager thread. An error was encountered in Music-on-Hold audio manager subcomponent while waiting for asynchronous event signaling. The MOH device will be restarted.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.

Cisco Unified CommunicationsRelease	Action
8.0(1)	This alarm is available in 8.0(1). • Severity changed from Error to Informational. • OS Error Description(String) parameter is added.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational

Parameter(s)

OS Error Description(String)

Recommended Action

No action is required.

kMOHMgrIsAudioSourceInUseThisIsNULL

Synchronization error detected in MOH audio manager. A synchronization error was detected. Condition has been resolved automatically.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1).

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational (6)

Recommended Action

No action is required.

kMOHRewindStreamControlNull

Attempted to rewind an inactive MOH audio source. An attempt was made to rewind or restart the Music-on-Hold audio source that is inactive. This has been ignored.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). • Severity changed from Error to Informational. • Audio Source ID [ULong] parameter is removed.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational

Parameters

Codec Type [String]

Recommended Action

None

kMOHRewindStreamMediaPositionObjectNull

Error rewinding MOH audio source that is not playing. An attempt was made to rewind or restart a Music-on-Hold wav file that was not being played. This has been ignored.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). • Severity changed from Error to Informational. • Audio Source ID [ULong] parameter is removed.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational

Parameters

Codec Type [String]

Recommended Action

None

kMTPDeviceStartingDefaults

One or more Cisco IP Voice Media Streaming App service parameter settings for the MTP device were not found in the database. The default values are included here.

History

Cisco Unified CommunicationsRelease	Action
3.x and 4.x	Added for Windows.
7.0(1)	Obsoleted.
8.0(1)	This alarm is available in 8.0(1). MTP Run Flag(String) parameter is added.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational (6)

Parameter(s)

MTP Run Flag(String)

Recommended Action

Configure the service parameter settings for the MTP device.

kReadCfgMOHEnabledCodecsNotFound

MOH enabled codecs not found. The Music-on-Hold service parameter for codec selection could not be read from database. Defaulting to G.711 mu-law codec.

Facility/Sub-Facility

CCM_MEDIA_STREAMING_APP-IPVMS

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

Informational (6)

Recommended Action

Set the Music-on-Hold service parameter for Cisco IP Voice Media Streaming App service.

LoadShareDeActivateTimeout

There was timeout during wait for DeActivateLoadShare acknowledgement.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Informational (6)

Recommended Action

None

LogFileSearchStringFound

The search string has been found in the log file. Trace and Log Central has found the search string that the user has configured.

Facility/Sub-Facility

CCM_TCT-LPMTCT

Cisco Unified Serviceability Alarm Definition Catalog

System/LpmTct

Severity

Informational (6)

Parameters

SearchString [String]

Recommended Action

If sysadmin is interested in collecting the traces around the time of generation of alert, use Trace and Log Central to collect the traces for that service.

MaxHoldDurationTimeout

A held call was cleared because the amount of time specified in the Maximum Hold Duration Timer service parameter had elapsed. If the allowed call-on-hold duration is too short, you can increase the value. If you do not want a limit on the duration of a held call, you can disable the limit.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	Following parameters added: • Originating Device Name(String) • Destination Device Name(String) • Hold start time(UInt) • Hold stop time(UInt) • Calling Party Number(String) • Called Party Number(String)

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational (6)

Parameters

Maximum Hold Duration (minutes) [Int]

Originating Device Name(String)

Destination Device Name(String)

Hold start time(UInt)

Hold stop time(UInt)

Calling Party Number(String)

Called Party Number(String)

Recommended Action

If the duration of the hold time is too short, increase the value in the Cisco CallManager service parameter or disable the maximum duration by setting the Maximum Hold Duration Timer parameter to zero.

PermissionDenied

An operation could not be completed because the process did not have authority to perform it.

Cisco Unified Serviceability Alarm Definition Catalog

System/Generic

Severity

Informational (6)

Parameters

None

Recommended Action

None

PktCapServiceStarted

Packet capture service started. Packet capture feature has been enabled on the Cisco Unified Communications Manager server. A Cisco CallManager service parameter, Packet Capture Enable, must be set to True for packet capture to occur.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational (6)

Recommended Action

None

PktCapServiceStopped

Packet capture service stopped. The packet capture feature has been disabled on the Cisco Unified Communications Manager server.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational (6)

Recommended Action

None

PktCapOnDeviceStarted

Packet capture started on the device. Indicated packet capture has been enabled on the device.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational (6)

Parameters

Device Name [String] Packet Capture Mode [String] Packet Capture Duration [String]

Recommended Action

None

PktCapOnDeviceStopped

Packet capture stopped on the device. Indicated packet capture has been disabled on the device.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational (6)

Parameters

Device Name [String] Packet Capture Mode [String] Packet Capture Duration [String]

Recommended Action

None

PublicationRunCompleted

Completion of publication of published DID patterns.

This alarm is generated when Unified CM completes a publication of the DID patterns into the IME network.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

INFORMATIONAL

Recommended Action

This alarm is provided for historic and informational purposes. It can be used to give you feedback that the system is working and is correctly publishing numbers into the IME network. It can also be used for troubleshooting. If some of the publishes fail for some reason, the alarm will contain a list of those numbers which were not published. If your users are receiving calls, and they are not over IP but you think they ought to be, you can check the history of these alarms to see if the number failed to be published into the network.

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Start time(String)

End time(String)

DID count(UInt)

Failed DID count(UInt)

Failed DIDs(String)

RedirectCallRequestFailed

CTIManager is unable to redirect a call

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CtiManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Directory Number(String)

Partition(String)

Recommended Action

This alarm is for informational purposes only; no action is required.

RollBackToPre8.0Disabled

Roll Back to Pre 8.0 has been disabled in the Enterprise Parameter page. This usually means that the RollBack to Pre 8.0 feature is modified in the Enterprise Parameter page.

Cisco Unified Serviceability Alarm Catalog

System/TVS

Severity

INFORMATIONAL

Routing List

SDI

Event Log

Data Collector

Sys Log

Recommended Action

None.

RollBackToPre8.0Enabled

Roll Back to Pre 8.0 has been enabled in the Enterprise Parameter page.

Cisco Unified Serviceability Alarm Catalog

System/TVS

Severity

INFORMATIONAL

Routing List

SDI

Event Log

Data Collector

Sys Log

Recommended Action

None.

RouteRemoved

Route removed automatically.

This alarm is generated when UC Manager removes a route from its routing tables because the route is stale and has expired, or because the far end has indicated the number is no longer reachable at that domain.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

E.164 number(String)

Domain name(String)

Route learned time(String)

Reason Code(Enum)

Recommended Action

This alarm is provided for historic and informational purposes. It helps you understand why certain numbers are in your routing tables, and why others are not. This historical information is useful to help determine why a call to a particular number is not going over IP, when you expect it to.

Related Topics

Reason Code Enum Definitions for RouteRemoved, on page 454

Reason Code Enum Definitions for RouteRemoved

Value	Definition
1	Expired
2	Unreachable

SAFPublishRevoke

A CLI command revoked the publish action for the specified service or subservice ID.

A system administrator issued a CLI command on the SAF Forwarder router to revoke the publish action for the service or subservice ID specified in this alarm.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

INFORMATIONAL

Routing List

SDL

SDI

Sys Log

Event Log

Parameter(s)

Client Handle(String)

Service ID(UInt)

Sub Service ID(UInt)

InstanceID1(UInt)

InstancID2(UInt)

InstanceID3(UInt)

InstanceID4(UInt)

Recommended Action

Informational purposes only; no action is required.

SAFUnknownService

Unified CM does not recognize the service ID in a publish revoke or withdraw message.

Unified CM received a Publish Revoke message or Withdraw message from the SAF Forwarder but the service ID in the message is not recognized by Unified CM. Unified CM may not recognize the service ID if the service ID was mistyped in the publish revoke CLI command, or if the service was previously withdrawn.

Cisco Unified Serviceability Alarm Catalog

CallManager/CallManager

Severity

Informational(6)

Routing List

SDL

SDI

Sys Log

Event Log

Parameters

Client Handle(String)

Service ID(UInt)

Sub Service ID(UInt)

InstanceID1(UInt)

InstancID2(UInt)

InstanceID3(UInt)

InstanceID4(UInt)

Recommended Action

None

SecurityEvent

Failed to write into the primary file path. Audit Event is generated by this application.

Cisco Unified Serviceability Alarm Catalog

AuditLog

Severity

INFORMATIONAL

Recommended Action

Ensure that the primary file path is valid and the corresponding drive has sufficient disk space. Also, make sure that the path has security permissions similar to default log file path.

ServiceActivated

This service is now activated.

Facility/Sub-Facility

CCM_SERVICEMANAGER-GENERIC

Cisco Unified Serviceability Alarm Definition Catalog

System/Service Manager

Severity

Informational (6)

Parameters

Service Name(String)

Recommended Action

None

ServiceDeactivated

The service is now deactivated.

Facility/Sub-Facility

CCM_SERVICEMANAGER-GENERIC

Cisco Unified Serviceability Alarm Definition Catalog

System/Service Manager

Severity

Informational (6)

Parameters

Service Name(String)

Recommended Action

None

ServiceStarted

Service has started.

History

Cisco Unified Communications ManagerRelease	Action
7.1	Added IPv6Address[Optional][String] parameter.

Facility/Sub-Facility

CCM_CBB-GENERIC

Cisco Unified Serviceability Alarm Definition Catalog

System/Generic

Severity

Informational (6)

Parameters

IP Address of hosting node(String)

IPV6Address[Optional](String)

Host name of hosting node(String)

Service Name(String)

Version Information(String)

Recommended Action

None

ServiceStopped

Service stopped.

Cisco Unified Serviceability Alarm Definition Catalog

System/Generic

Severity

Informational (6)

Parameters

IP Address of hosting node.(String)

Host of hosting node.(String)

Service (String)

Recommended Action

None

SoftwareLicenseValid

A valid software license has been detected by the IP Voice Media Streaming App service.

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/IpVms

Severity

INFORMATIONAL

Routing List

SDI

Event Log

Recommended Action

No action required. This informational message indicates alarm SoftwareLicenseNotValid is cleared.

StationAlarm

A station device sent an alarm to Cisco Unified Communications Manager, which acts as a conduit from the device to generate this alarm.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational (6)

Parameters

Protocol [String] TCP ProcessID [String] Device Text [String] Param1 [UInt] Param2 [UInt]

Recommended Action

Refer to the specific device type and information passed via this alarm to determine the appropriate action.

StationConnectionError

Station device is closing its connection with Cisco Unified Communications Manager because of the reason that is stated in this alarm.

History

Cisco Unified CommunicationsRelease	Action
8.0(1)	• Reason Code[Enum] parameter added. • Enum Definitions for Reason Code table added.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/CallManager

Severity

Informational

Parameters

Device Name [String]

Reason Code[Enum]

Related Topics

Reason Code Enum Definitions for StationConnectionError, on page 459

Reason Code Enum Definitions for StationConnectionError

Code	Reason
0	deviceInitiatedReset—The device has initiated a reset, possibly due to a power cycle or internal error. No action required; the device will reregister automatically.

Code	Reason
1	sccpDeviceThrottling—(SCCP only) The indicated SCCP device exceeded the maximum number of events allowed per-SCCP device. Events can be phone calls, KeepAlive messages, or excessive SCCP or non-SCCP messages. The maximum number of allowed events is controlled by the Cisco CallManager service parameter, Max Events Allowed. When an individual device exceeds the number configured in that service parameter, Unified CM closes the TCP connection to the device; automatic reregistration generally follows. This action is an attempt to stop malicious attacks on Unified CM or to ward off excessive CPU usage. No action necessary, the device will reregister automatically.
2	keepAliveTimeout—Unified CM did not receive a KeepAlive message from the device. Possible causes include device power outage, network power outage, network configuration error, network delay, packet drops and packet corruption. It is also possible to get this error if the Unified CM node is experiencing high CPU usage. Verify the device is powered up and operating, verify network connectivity between the device and Unified CM, and verify the CPU utilization is in the safe range (this can be monitored using RTMT via CPU Pegging Alert). No action necessary, the device will reregister automatically.
3	dbChangeNotify—An ApplyConfig command was invoked from Unified CM Administration resulting in an unregistration. No action necessary, the device will reregister automatically.
4	deviceRegistrationSuperceded—An initial device registration request was received but authentication had not yet completed before a new registration request was received. The first registration request was discarded and reregistration should proceed normally. No action is required, the device will reregister automatically.

Recommended Action

None

TestAlarmAppliance

Testing alarm for Appliance OS based server only.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Test

Severity

Informational (6)

Recommended Action

None

TestAlarmInformational

Testing informational alarm.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Test

Severity

Informational (6)

Recommended Action

None

TVSCertificateRegenerated

TVS Server certificate has been regenerated. This usually means that the TVS certificate has been regenerated. TVS server will automatically be restarted

Cisco Unified Serviceability Alarm Catalog

System/TVS

Severity

INFORMATIONAL

Routing List

SDI

Event Log

Data Collector

Sys Log

Recommended Action

None.

UserAlreadyLoggedIn

User is already logged in.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Informational (6)

Parameters

UserID [String]

Recommended Action

None

UserLoggedOut

User logged out.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Informational (6)

Parameters

UserID [String]

Recommended Action

None

UserLoginSuccess

User successfully logged in.

Facility/Sub-Facility

CCM_TCD-TCD

Cisco Unified Serviceability Alarm Definition Catalog

CallManager/TCD SRV

Severity

Informational (6)

Parameters

UserID [String]

Recommended Action

None

WDInformation

WebDialer informational alarm.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

Servlet Name [String] Reason [String]

Recommended Action

None

WDStarted

WebDialer Application started successfully.

Facility/Sub-Facility

CCM_JAVA_APPS-TOMCATAPPLICATIONS

Cisco Unified Serviceability Alarm Definition Catalog

System/Java Applications

Severity

Informational (6)

Parameters

Servlet Name [String] Reason [String]

Recommended Action

None

Debug-Level Alarms

The debug-level alarm is 7 and no action needed. Debug messages are used for troubleshooting.

TestAlarmDebug

Testing debug alarm.

Facility/Sub-Facility

CCM_CALLMANAGER-CALLMANAGER

Cisco Unified Serviceability Alarm Definition Catalog

System/Test

Severity

Debug (7)

Recommended Action

None

Cisco Unified Communications Manager Release 8.0(1) Obsolete Alarms

This section explains the alarms obsoleted in Cisco Unified Serviceability.

CallManager Catalog Obsolete Alarms

Alarm Name	Severity	Description
ConferenceCreated	INFORMATIONAL	An application controlled conference is created.
ConferenceDeleted	INFORMATIONAL	An application controlled conference is deleted.

Alarm Name	Severity	Description
CtiCallAcceptTimeout	WARNING	Call Accept Timeout
CtiStaleCallHandle	INFORMATIONAL	CTI stale call handle.
DatabaseAuditInfo_074	INFORMATIONAL	Database audit information.
DatabaseDeviceNoDirNum	NOTICE	No directory number for database device.
DatabaseInternalDataError_06e	ALERT	Database internal data error.
DatabaseInternalDataError_06f	NOTICE	Database internal data error.
DatabaseInternalDataError_070	INFORMATIONAL	Database internal data error.
DatabaseInternalDataError_071	INFORMATIONAL	Database internal data error.
DatabaseInternalDataError_072	INFORMATIONAL	Database internal data error.
DatabaseInternalDataError_073	INFORMATIONAL	Database internal data error.
DatabaseInternalDataError_075	INFORMATIONAL	Database internal data error.
DnTimeout	ERROR	DN Timeout.
GatewayAlarm	INFORMATIONAL	Gateway alarm.
H323AddressResolutionError	WARNING	H323 address not resolved.
H323CallFailureAlarm	WARNING	H323 Call failure
MWIParamMisMatch	WARNING	MWI parameter mismatch.
NoConnection	INFORMATIONAL	No TCP connection.
OutOfDnForAutoRegistration	WARNING	Out of directory numbers for auto-registration.
PktCapDownloadFailed	ERROR	Did not get captured packet or key file.
PktCapDownloadOK	INFORMATIONAL	Downloaded captured packet or key file.
PktCapLoginFailed	ERROR	Login failed for getting captured packet or key file.
PktCapLoginOK	INFORMATIONAL	Login OK for getting captured packet or key file.
Redirection	WARNING	Redirection Manager cannot register with the Call Control.

Alarm Name	Severity	Description
SIP IPPortConflict	WARNING	The local port for this device is already in use
ThrottlingSampleActivity	ERROR	ThrottlingSampleActivity
TotalCodeYellowEntry	INFORMATIONAL	TotalCodeYellowEntry

CertMonitor Alarm Catalog Obsolete Alarms

Alarm Name	Severity	Description
CertExpired	EMERGENCY	Certificate has Expired and needs to be changed at the earliest.
CertExpiryApproaching	INFORMATIONAL	Information Alarm that indicates a Certificate Validity Period is approaching and the expiry date is within the notification window configured.
CertExpiryDebug	DEBUG	Alarm to Debug Certificate Management.
CertExpiryError	ERROR	Alarm indicating errors in certificate Expiry Monitor Process.

CMI Alarm Catalog Obsolete Alarms

Alarm Name	Severity	Description
CCMConnectionError	ERROR	CMI cannot establish connection with the Cisco Unified Communications Manager.
CMIDebugAlarm	DEBUG	This alarm is generated only for the purpose of debugging.
CMIServiceStarted	NOTICE	Service is now running.
CMIServiceStopped	NOTICE	Service is now stopping.
COMException	ALERT	CMI catches an COM exception.
ConfigParaNotFound	NOTICE	CMI service configuration parameter is not found in Database.
DisconnectionToCCM	ERROR	CMI loses the connection with Unified Communications Manager.

Alarm Name	Severity	Description
WSAStartupFailed	CRITICAL	Windows Socket startup failed.

CTI Manager Alarm Catalog Obsolete Alarms

Alarm Name	Severity	Description
kCtiDeviceOpenFailAccessDenied	WARNING	DeviceOpenRequest failure.
kCtiDirectoryLoginFailure	WARNING	CTI directory login failure.
kCtiEnvProcDevListRegTimeout	ERROR	Directory change notification request time out.
kCtiExistingCallNotifyArrayOverflow	WARNING	Possible internal array overflow condition while generating CTI ExistingCall event.
kCtiIllegalEnumHandle	WARNING	Enumeration handle is not valid.
kCtiIllegalFilterSize	ERROR	ProviderOpenRequest; illegal filter size.
kCtiIllegalQbeHeader	ERROR	Illegal QBE header.
kCtiInvalidQbeSizeAndOffsets	ERROR	InvalidQBESizeAndOffsets; QBE message decoding encountered illegal size or offset.
kCtiLineCallInfoResArrayOverflow	WARNING	Possible internal array overflow condition while generating response to application request for call information.
kCtiLineOpenFailAccessDenied	WARNING	Line open failed.
kCtiMYTCPSendError	ERROR	MYTCP_Send: send error.
kCtiMytcpErrSocketBroken	WARNING	Socket connection has been broken.
kCtiNewCallNotifyArrayOverflow	WARNING	Possible internal array overflow condition while generating CTI NewCall event.
kCtiNullTcpHandle	WARNING	TranslateCtiQbeInputMessage: NULL TCP HANDLE!!! (QBE packet is dropped)
kCtiProviderOpenInvalidUserNameSize	ERROR	Invalid userName size in ProviderOpen request.
kCtiQbeLengthMisMatch	ERROR	OutputQbeMessage: length mismatch.
kCtiQbeMessageTooLong	WARNING	Incoming QBE message exceeds input buffer size

Alarm Name	Severity	Description
kCtiSdlErrorvException	CRITICAL	Failed to create an internal process that is required to service CTI applications.
kCtiSsRegisterManagerErr	ERROR	Unable to register CtiLine with SSAPI.
kCtiTcpInitError	ERROR	CTIManager service is unable to initialize TCP connection
kCtiUnknownConnectionHandle	WARNING	Connection handle is not valid

DB Alarm Catalog Obsolete Alarms

Alarm Name	Severity	Description
ErrorChangeNotifyReconcile	ALERT	A change notification shared memory reconciliation has occurred.

IpVms Alarm Catalog Obsolete Alarms

Alarm Name	Severity	Description
kANNAudioComException	ERROR	ANN TFTP COM exception
kANNAudioOpenFailed	ERROR	Open announcement file failed
kANNAudioTftpFileMissing	ERROR	ANN TFTP file missing
kANNAudioTftpMgrCreate	ERROR	Unable to create TFTP client
kANNAudioTftpMgrStartFailed	ERROR	TFTP start file transfer failed
kANNAudioThreadException	ERROR	ANN TFTP transfer exception failure
kANNAudioThreadWaitFailed	ERROR	ANN TFTP event wait error
kANNAudioThreadxFailed	ERROR	ANN TFTP transfer thread creation failed
kANNAudioXmlLoadFailed	ERROR	ANN XML parsing error
kANNAudioXmlSyntax	ERROR	ANN XML invalid element
kAddIpVmsRenderFailed	ERROR	Add IP VMS render filter-to-filter graph failure.

Alarm Name	Severity	Description
kCfgListComException	ERROR	Configuration COM Exception
kCfgListDblException	ERROR	Configuration DBL Exception
kCfgListUnknownException	ERROR	Unknown Configuration Exception
kCreateGraphManagerFailed	ERROR	Get graph manager failure.
kDeviceMgrThreadException	ERROR	Exception in device manager thread.
kDownloadMOHFileFailed	ERROR	Download request failure.
kFixedInputAddAudioCaptureDeviceFailed	ERROR	Add fixed audio source to filter graph failure.
kFixedInputAddG711AlawIpVmsRenderFailed	ERROR	Add fixed G711 a-law IP VMS render filter-to-filter graph failure.
kFixedInputAddG711UlawIpVmsRenderFailed	ERROR	Add fixed G711 ulaw IP VMS render filter to filter graph failed
kFixedInputAddG729IpVmsRenderFailed	ERROR	Add fixed G729 IP VMS render filter-to-filter graph failure.
kFixedInputAddMOHEncoderFailed	ERROR	Add fixed MOH encode filter-to-filter graph failure.
kFixedInputAddWideBandIpVmsRenderFailed	ERROR	Add fixed wideband IP VMS render filter-to-filter graph failure.
kFixedInputAudioCapMOHEncoderConnFailed	ERROR	Connect fixed audio capture device to MOH encoder failure.
kFixedInputAudioCaptureCreateFailed	ERROR	Get fixed system device enumerator failure.
kFixedInputClassEnumeratorCreateFailed	ERROR	Create fixed class enumerator failure.
kFixedInputCreateGraphManagerFailed	ERROR	Get fixed graph manager failure.
kFixedInputFindAudioCaptureDeviceFailed	ERROR	Unable to find fixed audio source device.
kFixedInputGetEventNotificationFailed	ERROR	Get fixed notification event failure.
kFixedInputGetFileNameFailed	ERROR	Get fixed audio source device name failure.
kFixedInputGetG711AlawIpVmsRendInfFailed	ERROR	Get fixed G711 a-law IP VMS render filter private interface failure.
kFixedInputGetG711AlawIpVmsRenderFailed	ERROR	Get fixed G711 a-law IP VMS render filter failure.

Alarm Name	Severity	Description
kFixedInputGetG711UlawIpVmsRendInfFailed	ERROR	Get fixed G711 mu-aw IP VMS render filter private interface failure.
kFixedInputGetG711UlawIpVmsRenderFailed	ERROR	Get fixed G711 mu-law IP VMS render filter failure.
kFixedInputGetG729IpVmsRendInfFailed	ERROR	Get fixed G729 IP VMS render filter private interface failure.
kFixedInputGetG729IpVmsRenderFailed	ERROR	Get fixed G729 IP VMS render filter failure.
kFixedInputGetMOHEncoderFailed	ERROR	Get fixed MOH encode filter failure.
kFixedInputGetMediaControlFailed	ERROR	Get fixed media control failure.
kFixedInputGetMediaPositionFailed	ERROR	Get fixed media position failure.
kFixedInputGetWideBandIpVmsRendInfFailed	ERROR	Get fixed wideband IP VMS render filter private interface failure.
kFixedInputGetWideBandIpVmsRenderFailed	ERROR	Get fixed wideband IP VMS render filter failure.
kFixedInputMOHEncG711AlawRenderConnFail	ERROR	Connect fixed MOH encoder to G711 a-law IP VMS render filter failure.
kFixedInputMOHEncG711UlawRenderConnFail	ERROR	Connect fixed MOH encoder to G711 u-law IP VMS render filter failure.
kFixedInputMOHEncG729RenderConnFailed	ERROR	Connect fixed MOH encoder to G729 IP VMS render filter failure.
kFixedInputMOHEncWidebandRenderConnFail	ERROR	Connect fixed MOH encoder to wideband IP VMS render filter failure.
kFixedInputSetNotifyWindowFailed	ERROR	Set fixed notify window failure.
kGetEventNotificationFailed	ERROR	Get notification event failure.
kGetIpVmsRenderFailed	ERROR	Get IP VMS render filter failure.
kGetIpVmsRenderInterfaceFailed	ERROR	Get IP VMS render filter private interface failure.
kGetMediaControlFailed	ERROR	Get media control failure.
kGetMediaPositionFailed	ERROR	Get media position failure.
kMOHFilterNotifyError	ERROR	Error on DirectShow returned or user abort.

Alarm Name	Severity	Description
kMOHMgrThreadCreateWindowExFailed	ERROR	Creation of MOH manager message window failure.
kMOHPlayStreamControlNull	ERROR	Stream Control pointer is NULL
kMOHPlayStreamMediaControlObjectNull	ERROR	Media Position COM interface is NULL
kMOHThreadException	ERROR	Exception in MOH manager thread.
kMTPICMPErrorNotification	INFORMATIONAL	MTP stream ICMP error.
kPWavMgrExitEventCreateFailed	ERROR	Creation of needed event failed.
kPWavMgrThreadException	ERROR	WAV file manager thread exception
kReadCfgANNComException	ERROR	COM error.
kReadCfgANNDblException	ERROR	Database exception.
kReadCfgANNListComException	ERROR	COM error.
kReadCfgANNListDblException	ERROR	Database exception.
kReadCfgANNListUnknownException	ERROR	Unknown exception.
kReadCfgANNUnknownException	ERROR	Unknown exception.
kReadCfgCFBComException	ERROR	COM error.
kReadCfgCFBDblException	ERROR	Database exception.
kReadCfgCFBListComException	ERROR	COM error.
kReadCfgCFBListDblException	ERROR	Database exception.
kReadCfgCFBListUnknownException	ERROR	Unknown exception.
kReadCfgCFBUnknownException	ERROR	Unknown exception.
kReadCfgDblGetChgNotifyFailed	INFORMATIONAL	Get change notification port failure.
kReadCfgDblGetNodeNameFailed	ERROR	Database layer select my process node failed.
kReadCfgEnterpriseComException	ERROR	COM error.
kReadCfgEnterpriseDblException	ERROR	Database exception.
kReadCfgEnterpriseException	ERROR	Enterprisewide configuration exception

Alarm Name	Severity	Description
kReadCfgEnterpriseUnknownException	ERROR	Unknown exception.
kReadCfgMOHAudioSourceComException	ERROR	COM error.
kReadCfgMOHAudioSourceDblException	ERROR	Database exception.
kReadCfgMOHAudioSourceUnknownException	ERROR	Unknown exception.
kReadCfgMOHComException	ERROR	COM error.
kReadCfgMOHDblException	ERROR	Database exception.
kReadCfgMOHListComException	ERROR	COM error.
kReadCfgMOHListDblException	ERROR	Database exception.
kReadCfgMOHListUnknownException	ERROR	Unknown exception.
kReadCfgMOHServerComException	ERROR	COM error.
kReadCfgMOHServerDblException	ERROR	Database exception.
kReadCfgMOHServerUnknownException	ERROR	Unknown exception.
kReadCfgMOHTFTIPAddressNotFound	ERROR	MOH TFTP IP address not found.
kReadCfgMOHUnknownException	ERROR	Unknown exception.
kReadCfgMTPComException	ERROR	COM error.
kReadCfgMTPDblException	ERROR	Database exception.
kReadCfgMTPListComException	ERROR	COM error.
kReadCfgMTPListDblException	ERROR	Database exception.
kReadCfgMTPListUnknownException	ERROR	Unknown exception.
kReadCfgMTPUnknownException	ERROR	Unknown exception.
kRenderFileFailed	ERROR	Render file-to-filter graph failure.
kSetNotifyWindowFailed	ERROR	Set notify window failure.

Test Alarm Catalog Obsolete Alarms

Alarm Name	Severity	Description
TestAlarmWindows	INFORMATIONAL	Testing INFORMATIONAL_ALARM.