Log in

System Error Messages for Cisco Unified Communications Manager

.og in to Save Content

Bias-Free Langua

Note

Optional parameter is indicated with the notation {Optional}. Application or Component may decide not to use that parameter in the alarm message.

Order of the parameters in an alarm message can change and it is decided by the Application or Component.

If the error message contains UNKNOWN_PARAMNAME, the parameter immediately following the UNKNOWN_PARAMNAME has not yet been updated in the alarm catalog. If this occurs, the error message is given a severity-level of 3, irrespective of the default severity-level for that error message.

Error Message

%UC_CMI-6-CMIServiceStatus: %[Priority=String][AppID=String][ClusterID=String] [NodeID=String]: Service is running and working properly.

Explanation CMI service is running and working properly.

Recommended Action Informational purpose only; no action is required.

Error Message

%UC_CMI-1-StopBitConfigurationError: %[StopBit=String][AppID=String][ClusterID=String] [NodeID=String]: The Cisco Messaging Interface service parameter, Stop Bits, has an invalid configuration.

Explanation 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 so that the value can be validated against the accepted range of values for this field.

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

Error Message

%UC_CMI-1-ParityConfigurationError: %[Parity=String][AppID=String][ClusterID=String] [NodeID=String]: The CMI service parameter, Parity, has an invalid configuration.

Explanation 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 so that the value can be validated against the accepted range of values for this field.

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

Error Message

%UC_CMI-5-SMDIMessageError: %[InvalidDN=String][AppID=String][ClusterID=String] [NodeID=String]: SMDI message contains invalid DN.

Explanation Some voice messaging systems send SMDI messages to Cisco Unified Communications Manager (Unified CM) with an invalid DN specifically for the purpose of verifying that Unified CM is functioning properly. In such cases, if the Validate DNs service parameter is set to True, CMI triggers this alarm because the DN cannot be found in the Unified CM database.

Recommended Action Verify that the Cisco Messaging Interface service parameter Validate DNs is set to false

Error Message

%UC_CMI-5-SMDICmdError: %[SMDICmd=String][AppID=String][ClusterID=String] [NodeID=String]: CMI receives an invalid incoming SMDI message.

Explanation There are two kinds of incoming messages that Cisco Unified Communications Manager can accept from the voice messaging system; they are OP:MWI(SP)nnnnnnn!(D) and RMV:MWI(SP)nnnnnnn!(D) (where:nnnnnnnnnn = station number (can be 7 or 10 digits), (D) = End Of Transmission, (SP) = space). The first message activates the message waiting indicator (MWI). The second deactivates the message waiting indicator. CMI triggers this alarm if the received MWI message doesn't have one of the acceptable formats as described.

Recommended Action Contact the vendor of the third-party voice messaging system and discover why it is sending SMDI message with an invalid format

Error Message

%UC_CMI-1-SerialPortOpeningError: %[OpeningError=String][AppID=String][ClusterID=String] [NodeID=String]: When CMI tries to open the serial port, the operating system returns an error.

Explanation 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.

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.

Error Message

%UC_CMI-3-SerialPortGetStatusError: %[GetStatusError=String][AppID=String][ClusterID=String] [NodeID=String]: When CMI tries to get the status of serial port, the operating system returns an error.

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

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

Error Message

%UC_CMI-3-SerialPortSetStatusError: %[SetStatusError=String][AppID=String][ClusterID=String][NodeID=String]: When CMI tries to set the status of serial port, the operating system returns an error.

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

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

Error Message

%UC_CMI-3-WritingFileFailure: %[ErrorInfo=String][AppID=String][ClusterID=String][NodeID=String]: CMI failed to write SMDI messages to the serial port.

Explanation CMI opened the serial port, however it failed to successfully write data 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.

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

Error Message

%UC_CMI-3-ReadingFileFailure: %[ErrorInfo=String][AppID=String][ClusterID=String][NodeID=String]: CMI failed to read SMDI messages from the serial port.

Explanation CMI opened the serial port, however it failed to successfully read data from 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.

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

Error Message

%UC_CMI-3-InvalidPortHandle: %[ErrorInfo=String][AppID=String][ClusterID=String][NodeID=String]: The handle for the opened serial port is invalid.

Explanation 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.

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

Error Message

%UC_CMI-1-VMDNConfigurationError: %[VoiceMailDN=String][AppID=String][ClusterID=String][NodeID=String]: The Voice Mail DN for CMI is invalid.

Explanation CMI can't 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 so that the value can be validated against the accepted range of values for this field.

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

Error Message

%UC_CMI-4-ThreadKillingError: %[ErrorInfo=String][AppID=String][ClusterID=String] [NodeID=String]: An error occurred when CMI tried to stop the CMI service.

Explanation As a normal part of the process of stopping the CMI service, open threads are closed (killed). This alarm indicates that a timeout occurred which means that the shutdown process is taking longer than expected, causing the operating system to return an error.

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).

Error Message

%UC_CMI-4-MemAllocFailed: %[MemAllocFailure=String][AppID=String][ClusterID=String] [NodeID=String]: CMI tried to allocate memory and failed.

Explanation 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.

Recommended Action Use the Real-Time Monitoring Tool to check 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).

Error Message

%UC_CMI-1-DBLException: %[DBLException=String][AppID=String][ClusterID=String] [NodeID=String]: Unable to connect to the DB.

Explanation When CMI service is started, it tries to read CMI Service Parameters from DB. During this, if CMI cannot connect to the database, it triggers this alarm.

Recommended Action Check Database connection, then restart CMI.

Error Message

%UC_CMI-1-CMIException: %[CMIException=String][AppID=String][ClusterID=String] [NodeID=String]: Error while reading the database.

Explanation 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.

Recommended Action Refer to the associated alarm for further information.

Error Message

%UC_CMI-1-UnknownException: %[AppID=String][ClusterID=String][NodeID=String]: Unknown error while connecting to DB.

Explanation 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.

Recommended Action Report to Customer Service representative.

Error Message

%UC_CMI-5-CMIServiceStarted: %[AppID=String][ClusterID=String][NodeID=String]: Service is now running.

Explanation CMI service has been started and running

Recommended Action Informational purpose only; no action is required

Error Message

%UC_CMI-5-CMIServiceStopped: %[AppID=String][ClusterID=String][NodeID=String]: Service is now stopping..

Explanation CMI Service has been stopped.

Recommended Action Informational purpose only; no action is required.

Error Message

%UC_CMI-7-CMIDebugAlarm: %[DebugMsg=String][AppID=String][ClusterID=String] [NodeID=String]: This alarm is generated only for the purpose of debugging.

Explanation CMI has several debug messages which simulate the real-time situations

Recommended Action Report to Customer Service representative

Error Message

%UC_CMI-3-CCMConnectionError: %[Cisco Unified Communications Manager Name=String] [AppID=String][ClusterID=String][NodeID=String]: CMI can't establish connection with the Cisco

Unified Communications Manager.

Explanation CMI can't establish connection with the Unified Communications Manager

Recommended Action Check the address/status of the CallManager and the network

Error Message

%UC_CMI-3-DisconnectionToCCM: %[Cisco Unified Communications Manager Name=String] [AppID=String][ClusterID=String][NodeID=String]: CMI loses the connection with Unified Communications Manager.

Explanation CMI loses the connection with the Cisco Unified Communications Manager

Recommended Action Check the status of the Unified Communications Manager and the Network

Error Message

%UC_CMI-2-WSAStartupFailed: %[ErrorInfo=String][AppID=String][ClusterID=String] [NodeID=String]: Windows Socket startup failed.

Explanation WinSock could not be started

Recommended Action Report to Customer Service representative.

Error Message

%UC_CMI-5-ConfigParaNotFound: %[ParaNameInfo=String][AppID=String][ClusterID=String] [NodeID=String]: CMI service configuration parameter is not found in Database.

Explanation CMI cannot find this process configuration parameter in process configuration table.

Recommended Action Report to Customer Service representative to get the database upgrade

Error Message

%UC_CMI-1-COMException: %[COMException=String][AppID=String][ClusterID=String] [NodeID=String]: CMI catches an COM exception..

Explanation CMI cannot find this process configuration parameter in process configuration table.

Recommended Action Check system setting and resource, then restart system.

Error Message

%UC_CTI-4-ApplicationConnectionDropped: %[LastPDUNumber=UInt][AppID=String] [ClusterID=String][NodeID=String]: Application has dropped the connection to CTIManager.

Explanation TCP or TLS connection between CTIManager and Application is disconnected

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)

Error Message

%UC_CTI-4-CtiMaxConnectionReached: %[AppID=String][ClusterID=String] [NodeID=String]: Maximum number of application connections is reached; application connection rejected.

Explanation Maximum number of CTI connections has been reached, no new connection will be accepted unless an existing connection is closed

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

Error Message

%UC_CTI-4-InvalidQBEMessage: %[CTIConnectionType=String][InstanceNumber=Long] [PDUNumber=Long][AppID=String][ClusterID=String][NodeID=String]: An invalid QBE PDU is received.

Explanation QBE PDU from application is invalid

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)

Error Message

%UC_CTI-3-CtiProviderOpenFailure: %[CTIconnectionId=Long][LoginUserId=String][Reason=Enum] [IPaddress=String][IPv6address=String][AppID=String][ClusterID=String][NodeID=String]: CTI application failed to open provider; application startup failed.

Explanation The application is unable to open provider. The IP address is shown in either IPv4 or IPv6 format depending on the Application's IP addressing mode

Recommended Action Review the reason code and the recommended action within the reason code

Reason Code - Enum Definitions

Enum Definitions - Reason

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 or 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 priviledges 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
0x8CCC011D (2362179869)	Directory login failed – Password expired. The user's login credentials have expired. The user can change the password by logging into the Cisco Unified CM User Options website using his/her existing credentials. The Cisco Unified CM User Options website will display the logon status indicating that the password has expired and will prompt the user to enter a new password
0x8CCC011F (2362179871)	Directory login failed – Account locked. A user has been

		locked out of his or her account. Lockouts can occur for one of the following reasons: 1) Too many tries: a user made too many login attempts using invalid credentials. Contact the user to confirm that he or she has been attempting to login. You can verify a user's login credential in Cisco Unified CM Administration (User Management > End User/Application User), select the User and click the Edit Credential button, then, under Credential Information, enable the Reset Hack Count checkbox to reset the hack count for this user and clear the Time Locked Due to Failed Login Attempts field. After the counter resets, notify the user that he or she can try logging in again. 2) Account locked by administrator: when warranted, an administrator can lockout a user's access. To do so, go to Cisco Unified CM Administration and click User Management > End User/Application User, select the user and click the Edit Credential button, then . To lock or unlock a user's account, under the Credential Information page, select or deselect the Locked by Administrator checkbox. 3) Account locked due to an extended period of inactivity: the Administrator must notify the user that his or her account has been locked due to inactivity. To unlock the user's

	account, the Administrator must change the password in Cisco Unified CM Administration by clicking under (User Management > End User/Application User), selecting the User and modifying the password in the End User/Application User Configuration window. After changing the password, notify the user about of his or her new password and encourage the user to change the password in Cisco Unified CM User Options to a new password of the user's choosing

Error Message

%UC_CTI-4-CtiQbeFailureResponse: %[ErrorCode=ULong][SeqNumber=Long] [ErrorMessageString=String][AppID=String][ClusterID=String][NodeID=String]: Requested operation from the application has failed.

Explanation The requested operation from the application could not be performed because of a normal or abnormal condition

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

Error Message

%UC_CTI-6-CtiProviderClosed: %[LoginUserId=String][SeqNumber=Long][CTIconnectionId=Long] [IPAddress=String][IPv6Address=String][Reason=Enum][AppID=String][ClusterID=String] [NodeID=String]: CTI application connection has been closed.

Explanation Application closed the provider. The IP address is shown in either IPv4 or IPv6 format depending on the Application's IP addressing mode

Recommended Action This alarm is for informational purposes only; no action is required.

Reason Code - Enum Definitions

Enum Definitions - Reason

Value	Definition
0	Unknown
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 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
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

Error Message

%UC_CTI-6-CtiProviderOpened: %[LoginUserId=String][SeqNumber=Long][Version=String][CTIconnectionId=Long][IPAddress=String][IPv6Address=String][CmAssignedAppID=Long][AppID=String][ClusterID=String][NodeID=String]: CTI application connection opened..

Explanation Application opened the provider successfully. The IP address is shown in either IPv4 or IPv6 format depending on the Application's IP addressing mode.

Recommended Action This alarm is for informational purposes only; no action is required.

Error Message

%UC_CTI-3-UnableToRegisterwithCallManagerService: %[CmNodeID=Long][AppID=String][ClusterID=String][NodeID=String]: Unable to communicate with the Cisco CallManager service.

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

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

Error Message

%UC_CTI-4-CtiProviderCloseHeartbeatTimeout: %[AppID=String][ClusterID=String][NodeID=String]: CTI heartbeat timed out; application disconnected.

Explanation CTI heartbeat timeout occurred causing CTIManager to close the application connection

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

Error Message

%UC_CTI-4-CtiProviderClosePeerCertExpired: %[AppID=String][ClusterID=String] [NodeID=String]: CTI Peer Certificate Expired; Application Disconnected.

Explanation CTI Peer certificate expired causing CTIManager to close the application connection

Recommended Action The validity period of the peer certificate used for making SSL connection is expired. Please update the certificate

Error Message

%UC_CTI-4-CtiProviderPeerCertExpireSoon: %[AppID=String][ClusterID=String][NodeID=String]: CTI Peer Certificate will expire soon; If expired, application will disconnect.

Explanation CTI Peer certificate expire soon.

Recommended Action The validity period of the peer certificate used for making SSL connection will expire soon. Please update the new certificate for getting continous service

Error Message

%UC_CTI-4-CtiIncompatibleProtocolVersion: %[MsgVersion=VoidPtr][CompatibleVersions=VoidPtr] [CurrentVersion=VoidPtr][CMVersion=String][IPAddress=String][IPv6Address=String][AppID=String] [ClusterID=String][NodeID=String]: Incompatible protocol version.

Explanation 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 Application's IP addressing mode

Recommended Action Verify that the correct version of the application is being used. If you're unsure 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)

Error Message

%UC_CTI-6-CtiDeviceOpened: %[DeviceName=String][SeqNumber=Long][DeviceId=Long] [DeviceType=Long][CTIconnectionId=Long][MediaControlled=Bool][AssociatedCMIPAddr=String] [CmAssignedAppID=Long][AppID=String][ClusterID=String][NodeID=String]: Device opened.

Explanation Application opened a device

Recommended Action This alarm is for informational purposes only; no action is required

Error Message

%UC_CTI-6-CtiDeviceClosed: %[DeviceName=String][DeviceId=Long][DeviceType=Long] [CTIconnectionId=Long][MediaControlled=Bool][AssociatedCMIpAddr=String][Reason=Enum] [AppID=String][ClusterID=String][NodeID=String]: Device closed.

Explanation Application closed a device

Recommended Action This alarm is for informational purposes only; no action is required

Reason Code - Enum Definitions

Enum Definitions - Reason

Value	Definition

0	Unknown
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 dyamic 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	Unsuppported device configuration
18	Device is being reset
19	IPAddress mode does not match what is configured in Unified CM

Error Message

%UC_CTI-4-CtiDeviceOpenFailure: %[CTIconnectionId=Long][DeviceName=String][Reason=Enum][AppID=String][ClusterID=String][NodeID=String]: Device Open failed.

Explanation Application is unable to open the device

Recommended Action Check the reason code and take appropriate action to resolve the issue

Reason Code - Enum Definitions

Enum Definitions - Reason

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)

Error Message

%UC_CTI-6-CtiDeviceOutofService: %[DeviceId=Long][CTIconnectionId=Long][DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: Device is out of service.

Explanation Device is out of service

Recommended Action This alarm is for informational purposes only; no action is required

Error Message

%UC_CTI-6-CtiDeviceInService: %[DeviceId=Long][CTIconnectionId=Long][DeviceName=String][callManagerId=Long][AppID=String][ClusterID=String][NodeID=String]: Device in service..

Explanation Device is back in service

Recommended Action This alarm is for informational purposes only; no action is required

Error Message

%UC_CTI-6-CtiLineOpened: %[SeqNumber=Long][DirNum=String][Partition=String][DeviceName=String][CTIconnectionId=Long][AppID=String][ClusterID=String][NodeID=String]: Line opened.

Explanation Application opened the line

Recommended Action This alarm is for informational purposes only; no action is required

Error Message

%UC_CTI-4-CtiLineOpenFailure: %[CTIconnectionId=Long][DeviceName=String][DirNum=String][Partition=String][Reason=Enum][AppID=String][ClusterID=String][NodeID=String]: Unable to open the line.

Explanation Application is unable to open the line

Recommended Action Review the reason code and take appropriate action to resolve the issue

Reason Code - Enum Definitions

Enum Definitions - Reason

Value	Definition
0	Unknown
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

Error Message

%UC_CTI-6-CtiLineClosed: %[DirNum=String][Partition=String][CTIconnectionId=Long] [DeviceName=String][Reason=Enum][AppID=String][ClusterID=String][NodeID=String]: Line closed..

Explanation Application closed the line

Recommended Action This alarm is for informational purposes only; no action is required

Reason Code - Enum Definitions

Enum Definitions - Reason

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
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	Unsuppported device configuration

Error Message

%UC_CTI-6-CtiLineOutOfService: %[DirNum=String][Partition=String][CTIconnectionId=Long] [DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: Line is out of service.

Explanation Line is going out of service

Recommended Action This alarm is for informational purposes only; no action is required

Error Message

%UC_CTI-6-CtiLineInService: %[LineId=Long][CTIconnectionId=Long][AppID=String] [ClusterID=String][NodeID=String]: Line in service.

Explanation Line is back in service

Recommended Action This alarm is for informational purposes only; no action is required

Error Message

%UC_CTI-4-UnableToSetorResetMWI: %[DirNum=String][AppID=String][ClusterID=String] [NodeID=String]: Error in setting message waiting indicator.

Explanation An error occurred when setting the message waiting indication (MWI) lamp

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

Error Message

%UC_CTI-6-RedirectCallRequestFailed: %[SeqNumber=Long][DirNum=String][Partition=String] [AppID=String][ClusterID=String][NodeID=String]: Request from application to redirect a call has failed.

Explanation CTIManager is unable to redirect a call

Recommended Action This alarm is for informational purposes only; no action is required

Error Message

%UC_CTI-4-MaxDevicesPerProviderExceeded: %[AppID=String][ClusterID=String] [NodeID=String]: Application has opened more devices than allowed.

Explanation An application has opened more devices than the limit set in the CTIManager service parameter, Maximum Devices Per Provider

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

Error Message

%UC_CTI-4-MaxDevicesPerNodeExceeded: %[AppID=String][ClusterID=String] [NodeID=String]: Application has opened more devices than the limit for each node.

Explanation An application has opened more devices than the limit set in the CTIManager service parameter, Maximum Devices Per Node.

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

Error Message

%UC_CTI-4-ApplicationConnectionError: %[CTIConnectionType=String][InstanceNumber=Long] [AppID=String][ClusterID=String][NodeID=String]: CTIManager is unable to allow connections from Applications..

Explanation CTIManager is unable to accept connections from applications

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

Error Message

%UC_CTI-3-kCtiQbeLengthMisMatch: %[AppID=String][ClusterID=String] [NodeID=String]: OutputQbeMessage: length mismatch..

Explanation QBE header length mismatch exists.

Recommended Action This alarm indicates that TSP/JTAPI is incompatible with the version of 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).

Error Message

%UC_CTI-3-kCtiInvalidQbeSizeAndOffsets: %[AppID=String][ClusterID=String] [NodeID=String]: InvalidQBESizeAndOffsets; QBE message decoding encountered illegal size or offset..

Explanation QBE Packet received from the application is not encoded correctly.

Recommended Action A TSP/JTAPI interface error occurred; the QBE message may not be formatted correctly. TSP/JTAPI might be incompatible with the version of CTIManager. Install the JTAPI or TSP plugin (Cisco Unified CM Administration > Application > Plugins) and restart the application.

Error Message

%UC_CTI-3-kCtiSsRegisterManagerErr: %[AppID=String][ClusterID=String][NodeID=String]: Unable to register CtiLine with SSAPI..

Explanation CTI cannot register CtiLine with SSAPI.

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.

Error Message

%UC_CTI-4-kCtiMytcpErrSocketBroken: %[AppID=String][ClusterID=String][NodeID=String]: Socket connection has been broken..

Explanation The TCP connection has been lost.

Recommended Action Although connection to the application is lost, no action is required if lost connection was intentional. If loss of connectivity was unintentional, investigate what might have caused connectivity to be lost and restore the connection.

Error Message

%UC_CTI-4-kCtiDirectoryLoginFailure: %[SeqNumber=Long][AppID=String][ClusterID=String][NodeID=String]: CTI directory login failure..

Explanation CTI Manager is unable to login to directory. As a result, the application may not be able to access the controlled device list.

Recommended Action In Cisco Unified CM Administration, verify that the correct username and password has been configured and is being used for CTIManager login. If LDAP is used for authentication, check to confirm that the LDAP synchronization is configured and is working.

Error Message

%UC_CTI-4-kCtiDeviceOpenFailAccessDenied: %[LoginUserId=String][DeviceName=String][DeviceType=Long][AppID=String][ClusterID=String][NodeID=String]: DeviceOpenRequest failure..

Explanation Application is trying to access a device that is not in its control.

Recommended Action Check the application sending the request or add the device to the user control list.

Error Message

%UC_CTI-3-kCtiIllegalQbeHeader: %[AppID=String][ClusterID=String][NodeID=String]: Illegal QBE header..

Explanation Because of illegal QBE header, QBE message has been rejected.

Recommended Action QBE header could be fragmented due to TCP fragmentation. Review your network configuration to fix any TCP fragmentation issue.

Error Message

%UC_CTI-4-kCtiLineOpenFailAccessDenied: %[SeqNumber=Int][DirNum=String][Partition=String][DeviceName=String][UserName=String][AppID=String][ClusterID=String][NodeID=String]: Line open failed..

Explanation Application failed to open a line.

Recommended Action Add the device associated with the line to the user device control list.

Error Message

%UC_CTI-4-kCtiIllegalEnumHandle: %[EnumHandle=Long][EnumObjectType=String][AppID=String][ClusterID=String][NodeID=String]: Enumeration handle is not valid..

Explanation The enumeration handle associated with the process of enumerating devices, lines or DNs is invalid.

Recommended Action Check whether all devices, lines or DNs configured for the application are available to the application. 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).

Error Message

%UC_CTI-4-kCtiQbeMessageTooLong: %[CTIConnectionType=String][InstanceNumber=Long] [QBEMessageLength=Long][AppID=String][ClusterID=String][NodeID=String]: Incoming QBE message exceeds input buffer size.

Explanation An incoming QBE message exceeds the input buffer size and then gets dropped.

Recommended Action The size of the QBE packet could exceed the suggested size when the JTAPI/TSP version is not compatible with the version of CTIManager. Contact the application vendor and verify that the application is compatible with the version of Cisco Unified Communications Manager (Unified CM). If the application vendor requests you to, install the JTAPI or TSP plugin (Cisco Unified CM Administration > Application > Plugins) and restart the application.

Error Message

%UC_CTI-4-kCtiNullTcpHandle: %[PDU_Number=Long][AppID=String][ClusterID=String] [NodeID=String]: TranslateCtiQbeInputMessage: NULL TCP HANDLE!!! (QBE packet is dropped).

Explanation A null TCP handle is preventing the QBE packets to be reported to applications.

Recommended Action This problem typically happens due to a network connectivity failure. Check for and resolve any connectivity issues in your network.

Error Message

%UC_CTI-3-kCtiEnvProcDevListRegTimeout: %[AppID=String][ClusterID=String] [NodeID=String]: Directory change notification request time out..

Explanation CTIManager registration request to EnvProcDevList timed out; CTIManager will send another registration request.

Recommended Action Check and resolve network connectivity problems between Cisco Unified Communications Manager nodes.

Error Message

%UC_CTI-3-kCtiMYTCPSendError: %[AppID=String][ClusterID=String][NodeID=String]: MYTCP_Send: send error..

Explanation TCP socket connection has been broken.

Recommended Action This problem occurs when an application is abruptly shut down or has lost network connectivity to CTIManager. Review your application and network connectivity and resolve any issues.

Error Message

%UC_CTI-2-kCtiSdlErrorvException: %[AppID=String][ClusterID=String][NodeID=String]: Failed to create an internal process that is required to service CTI applications..

Explanation An unexpected internal SDL error caused a failure in creating CTIManager Service SDL Process.

Recommended Action An internal CTIManager error has occurred. Try Restarting the CTIManager service to resolve this problem, if it does resolve the problem restart the Unified CM Server.

Error Message

%UC_CTI-3-kCtiTcpInitError: %[ErrorCode=Int][AppID=String][ClusterID=String]
[NodeID=String]: CTIManager service is unable to initialize TCP connection.

Explanation CTIManager service is unable to initialize TCP connection

Recommended Action CTIManager has encountered difficulty initializing TCP connections. Restart the CTIManager service to resolve this problem.

Error Message

%UC_CTI-3-kCtiIllegalFilterSize: %[AppID=String][ClusterID=String]
[NodeID=String]: ProviderOpenRequest; illegal filter size..

Explanation ProviderOpenRequest has an illegal filter size.

Recommended Action The application is using an incompatible version of JTAPI/TSP and Cisco Unified Communications Manager. Install the JTAPI or TSP plugin (Cisco Unified CM Administration > Application > Plugins) and restart the application.

Error Message

%UC_CTI-4-kCtiNewCallNotifyArrayOverflow: %[AppID=String][ClusterID=String]
[NodeID=String]: Possible internal array overflow condition while generating CTI NewCall event..

Explanation An unexpected internal error occurred.

Recommended Action Restart the CTIManager service if the problem persists.

Error Message

%UC_CTI-4-kCtiExistingCallNotifyArrayOverflow: %[AppID=String][ClusterID=String]
[NodeID=String]: Possible internal array overflow condition while generating CTI ExistingCall event..

Explanation An unexpected internal error occurred.

Recommended Action Restart the CTIManager service if the problem persists.

Error Message

%UC_CTI-4-kCtiLineCallInfoResArrayOverflow: %[AppID=String][ClusterID=String]
[NodeID=String]: Possible internal array overflow condition while generating response to application request for call information..

Explanation An unexpected internal error occurred.

Recommended Action Restart the CTIManager service if the problem persists.

Error Message

%UC_CTI-4-kCtiUnknownConnectionHandle: %[CTIConnectionType=String][InstanceNumber=Long]
[AppID=String][ClusterID=String][NodeID=String]: Connection handle is not valid..

Explanation A message has been received from an unknown connection, and then dropped.

Recommended Action This alarm occurs when a QBE packet is received from a connection that is already disconnected. This packet will be ignored by CTIManager and no action is required.

Error Message

%UC_CTI-3-kCtiProviderOpenInvalidUserNameSize: %[UserNameSize=Long][AppID=String][ClusterID=String][NodeID=String]: Invalid userName size in ProviderOpen request..

Explanation User name length is invalid.

Recommended Action Ask user of CTI application to use correct userName and to check the user name in configuration. It should not be more than 31 characters.

Error Message

%UC_DB-3-kDbConnectionFailed: %[AdditionalInfo=String][AppID=String][ClusterID=String][NodeID=String]: Database connection failed..

Explanation An attempt to connect to database failed.

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

Error Message

%UC_DB-1-NoDbConnectionAvailable: %[AppID=String][ClusterID=String][NodeID=String]: No database connection available..

Explanation Database layer could not find any working database connection.

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.

Error Message

%UC_DB-2-ErrorChangeNotifyClientBlock: %[AppID=String][ClusterID=String][NodeID=String]: 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..

Explanation 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.

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 error messages that may have occurred around the time of the alarm.

Error Message

%UC_DB-3-ErrorReadingInstalledRPMS: %[AppID=String][ClusterID=String][NodeID=String]: Could not read installed RPMs to populate component version table.

Explanation The function that reads the rpm version information and populates database failed

Recommended Action Please report this error to the administrator.

Error Message

%UC_DB-3-ErrorChangeNotifyClientTimeout: %[AppID=String][ClusterID=String][NodeID=String]: A change notification client was responding slowly and has been removed..

Explanation A change notification recipient hasn't responded to change notification in several minutes and was thus removed. This may delay call processing features, such as call forwarding and so on.

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.

Error Message

%UC_DB-1-ErrorChangeNotifyReconcile: %[AppID=String][ClusterID=String][NodeID=String]: A change notification shared memory reconciliation has occurred..

Explanation The change notification buffers in shared memory have been rebuilt due to conflicts.

Recommended Action This problem may have been already corrected. If unexpected behavior is observed, restart all Cisco services in the cluster.

Error Message

%UC_DB-6-IDSEngineDebug: %[class_id=String][class_msg=String][specific_msg=String] [AppID=String][ClusterID=String][NodeID=String]: Indicates debug events from IDS database engine..

Explanation This alarm provides low-level debugging information from IDS database engine. System administrator can disregard this alarm.

Recommended Action This is for debug information purposes only; no action is required.

Error Message

%UC_DB-1-IDSEngineAttention: %[class_id=String][class_msg=String][specific_msg=String] [AppID=String][ClusterID=String][NodeID=String]: Information about IDS replication

Explanation This alarm provides information about IDS replication and cluster network connectivity.

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

Error Message

%UC_DB-6-IDSEngineInformation: %[class_id=String][class_msg=String][specific_msg=String] [AppID=String][ClusterID=String][NodeID=String]: No error has occurred but some routine event completed in IDS database engine..

Explanation This alarm is informational. No error has occurred but some routine event completed in IDS database engine.

Recommended Action This is for information purposes only; no action is required.

Error Message

%UC_DB-3-IDSEngineCritical: %[class_id=String][class_msg=String][specific_msg=String] [AppID=String][ClusterID=String][NodeID=String]: Pay Attention. This alarm does not compromise data or prevent the use of the system..

Explanation Pay Attention. This alarm does not compromise data or prevent the use of the system.

Recommended Action This alarm needs monitoring by the db admin

Error Message

%UC_DB-3-IDSEngineFailure: %[class_id=String][class_msg=String][specific_msg=String] [AppID=String][ClusterID=String][NodeID=String]: Combined alarm for emergency and error situations. Something unexpected occurred that might compromise data or access to data or cause IDS to fail.

Explanation 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

Recommended Action Requires db admin intervention

Error Message

%UC_DB-6-IDSReplicationInformation: %[class_id=String][class_msg=String][specific_msg=String] [AppID=String][ClusterID=String][NodeID=String]: Information about IDS replication.

Explanation This alarm provides information about IDS replication.

Recommended Action Informational purposes only; no action is required

Error Message

%UC_DB-3-IDSReplicationFailure: %[class_id=String][class_msg=String][specific_msg=String] [AppID=String][ClusterID=String][NodeID=String]: Combined alarm for emergency and error situations. IDS Replication has failed.

Explanation This alarm indicates combined alarm for emergency and error situations. It indicates failure in IDS Replication

Recommended Action Requires db admin intervention

Error Message

%UC_DB-3-CUPImportFailure: %[class_id=String][class_msg=String][specific_msg=String] [AppID=String][ClusterID=String][NodeID=String]: Combined alarm for Integration, CUP import files has failed.

Explanation Combined alarm for Integration, CUP import files has failed

Recommended Action Check the network and files in the CUP server

Error Message

%UC_DB-3-DBUserLimitExceeded: %[user=String][AppID=String][ClusterID=String] [NodeID=String]: An application or endpoint is using too many database resources.

Explanation This alarm indicates an error situation. Resources are not exhausted. The application will not be granted more connections to the database until the ones used are freed up.

Recommended Action Collect the trace using file get activelog cm/trace/dbl/sdi/limitexceeded*.tar.gz or by collecting the Cisco Database Layer Monitor trace in RTMT to determine the application or endpoint causing issues.

Error Message

%UC_GENERIC-0-OutOfMemory: %[AppID=String][ClusterID=String][NodeID=String]: Out of memory..

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

Recommended Action No action is required.

Error Message

%UC_GENERIC-6-PermissionDenied: %[AppID=String][ClusterID=String][NodeID=String]: Permission has been denied..

Explanation An operation could not be completed because the process did not have authority to perform it.

Recommended Action This alarm is for information purposes only; no action is required.

Error Message

%UC_GENERIC-0-ServiceNotInstalled: %[ServiceName=String][AppID=String][ClusterID=String] [NodeID=String]: Service is not installed..

Explanation An executable is trying to start but cannot because it is not configured as a service in the service control manager.

Recommended Action Reinstall the service.

Error Message

%UC_GENERIC-6-ServiceStopped: %[IPAddress=String][Hostname=String][ServiceName=String] [ProcessID=ULong][AppID=String][ClusterID=String][NodeID=String]: Service stopped..

Explanation A service has stopped.

Recommended Action This alarm is for information purposes only; no action is required.

Error Message

%UC_GENERIC-6-ServiceStarted: %[ProcessID=ULong][IPAddress=String][IPV6Address=String] [Hostname=String][ServiceName=String][VersionInfo=String][AppID=String][ClusterID=String] [NodeID=String]: Service started..

Explanation A service has started.

Recommended Action This alarm is for information purposes only; no action is required.

Error Message

%UC_GENERIC-4-ServiceStartupFailed: %[ServiceName=String][AppID=String][ClusterID=String] [NodeID=String]: Service startup failure..

Explanation An attempt to start the specified service failed.

Recommended Action Restart the service.

Error Message

%UC_GENERIC-0-FileWriteError: %[PrimaryFilePath=String][AppID=String][ClusterID=String] [NodeID=String]: Cannot write into a file..

Explanation Failed to write into the primary file path.

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.

Error Message

%UC_GENERIC-3-CipherListXmlParsingFailed: %[ErrorMsg=String][XmlFileParsed=String] [AppID=String][ClusterID=String][NodeID=String]: The system was unable to parse the cipher list for all interfaces.

Explanation This Alarm Indicates that there was a failure parsing the list of supported ciphers.

Recommended Action Try saving the Cipher Control List in Operating Systems Administration or deleting the ciphers configured from all interfaces then restart the system and reconfigure the desired cipher control list. If this issue persists contact Cisco Technical Assistance Center (TAC) for further support.

Error Message

%UC_GENERIC-6-CiphersConfiguredForanInterfaceApplied: %[InterfaceConfigured=String] [AppID=String][ClusterID=String][NodeID=String]: Security ciphers configured for the configured Interface have been applied.

Explanation This alarm indicates a new cipher list has been applied to the interface as a result of a UI change to the configured ciphers followed by a service restart.

Recommended Action Check the application logs for the interface to find details of the ciphers configured.

Error Message

%UC_IPVMS-3-kReadCfgUserLocaleEnterpriseSvcParm: %[AppID=String][ClusterID=String] [NodeID=String]: Error reading enterprise default user locale configuration.

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

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.

Error Message

%UC_IPVMS-6-kANNICMPErrorNotification: %[CID=ULong][PID=ULong][IP=String][Port=ULong] [AppID=String][ClusterID=String][NodeID=String]: ANN stream ICMP port unreachable error..

Explanation 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.

Recommended Action No action is required. This may occur at times when connections are being stopped or redirected.

Error Message

%UC_IPVMS-6-kIVRDICMPErrorNotification: %[CID=ULong][PID=ULong][IP=String][Port=ULong] [AppID=String][ClusterID=String][NodeID=String]: IVR stream ICMP port unreachable error.

Explanation 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.

Recommended Action No action is required. This may occur at times when connections are being stopped or redirected.

Error Message

%UC_IPVMS-6-kMTPICMPErrorNotification: %[CID=ULong][PID=ULong][IP=String][Port=ULong][AppID=String][ClusterID=String][NodeID=String]: MTP stream ICMP port unreachable error.

Explanation 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.

Recommended Action No action is required. This may occur at times when connections are being stopped or redirected.

Error Message

%UC_IPVMS-3-kANNDeviceRecordNotFound: %[AppID=String][ClusterID=String][NodeID=String]: ANN device record not found..

Explanation 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.

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

Error Message

%UC_IPVMS-3-kIVRDeviceRecordNotFound: %[AppID=String][ClusterID=String][NodeID=String]: IVR device record not found.

Explanation A device record for the interactive voice response device was not found in the database. The IVR device is normally automatically added when the server is added to the database.

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

Error Message

%UC_IPVMS-3-kPWavMgrThreadxFailed: %[Error=ULong][ErrorText=String][AppID=String] [ClusterID=String][NodeID=String]: WAV playing manager thread creation failed.

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

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

Error Message

%UC_IPVMS-3-ANNDeviceRecoveryCreateFailed: %[Error=Int][ErrorText=String][AppID=String] [ClusterID=String][NodeID=String]: ANN device recovery create failure..

Explanation The ANN 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 announcement device will not be available.

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

Error Message

%UC_IPVMS-3-IVRDeviceRecoveryCreateFailed: %[Error=Int][ErrorText=String][AppID=String] [ClusterID=String][NodeID=String]: IVR device recovery create failure.

Explanation The IVR 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 interactive voice response device will not be available.

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

Error Message

%UC_IPVMS-3-kReadCfgANNListUnknownException: %[DeviceName=String][AppID=String] [ClusterID=String][NodeID=String]: Unknown exception..

Explanation An unknown exception occurred while trying to read ANN device Cisco Unified Communications Manager list information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgANNListComException: %[DeviceName=String][Description=String] [AppID=String][ClusterID=String][NodeID=String]: COM error..

Explanation A COM error occurred while trying to read ANN device Cisco Unified Communications Manager list information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgANNListDbIException: %[DeviceName=String][ExceptionStr=String] [ExceptionID=ULong][AppID=String][ClusterID=String][NodeID=String]: Database exception..

Explanation A database exception occurred while trying to read ANN device Cisco Unified Communications Manager list information.

Recommended Action Device will not start; fix database problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgANNUnknownException: %[DeviceName=String][AppID=String]

[ClusterID=String][NodeID=String]: Unknown exception..

Explanation An unknown exception occurred while trying to read ANN device configuration information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgANNComException: %[DeviceName=String][Description=String] [AppID=String][ClusterID=String][NodeID=String]: COM error..

Explanation A COM error occurred while trying to read ANN device configuration information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgANNDblException: %[DeviceName=String][ExceptionStr=String] [ExceptionID=ULong][AppID=String][ClusterID=String][NodeID=String]: Database exception..

Explanation A database exception occurred while trying to read ANN device configuration information.

Recommended Action Device will not start; fix database problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgEnterpriseException: %[AppID=String][ClusterID=String] [NodeID=String]: Enterprisewide configuration exception.

Explanation An unknown exception occured reading Enterjprisewide configuration settings.

Recommended Action Verify the enterprise configuration settings and restart the IP Media Streaming Service.

Error Message

%UC_IPVMS-3-kCfgListUnknownException: %[AppID=String][ClusterID=String] [NodeID=String]: Unknown Configuration Exception.

Explanation An exception error was generated reading the service parameter settings.

Recommended Action Restart the server.

Error Message

%UC_IPVMS-3-kCfgListComException: %[Description=String][AppID=String][ClusterID=String] [NodeID=String]: Configuration COM Exception.

Explanation A COM exception error was generated reading the service parameter settings for devices.

Recommended Action Verify that service parameters can be viewed using CCM Administration. If they can then restart the service or server.

Error Message

%UC_IPVMS-3-kCfgListDblException: %[Description=String][ExceptionID=ULong][AppID=String] [ClusterID=String][NodeID=String]: Configuration DBL Exception.

Explanation An exception error was generated reading the service parameter settings for devices.

Recommended Action Verify that service parameters can be viewed using CCM Administration. If they can then restart the service or server.

Error Message

%UC_IPVMS-4-kANNDeviceStartingDefaults: %[Field=String][Value=String][AppID=String][ClusterID=String][NodeID=String]: ANN device configuration not found.

Explanation 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.

Recommended Action Review the service parameter settings and configure the ANN device settings properly using the CUCM Administration.

Error Message

%UC_IPVMS-3-kRequestedANNStreamsFailed: %[Requested=ULong][Allocated=ULong][AppID=String][ClusterID=String][NodeID=String]: ANN requested streams failure..

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

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

Error Message

%UC_IPVMS-3-kRequestedIVRStreamsFailed: %[Requested=ULong][Allocated=ULong][AppID=String][ClusterID=String][NodeID=String]: IVR requested streams failure.

Explanation The requested resources for the configured number of IVR calls (Call Count service parameter) was not available. If the value shown as "Allocated" is non-zero

Recommended Action Verify the IVR Call Count service parameter is correct. A server restart may be needed to recover resources.The total capacity of stream resources may have been exceeded by a combi nation of settings for SW Conference Bridge, Music on Hold, SW Media Termination Point, Annunciator, or the Self Provisioning service. To increase the IVR calls may require reducing one of the other media device resource settings.

Error Message

%UC_IPVMS-4-kANNAudioCreateDirFailed: %[Error=ULong][ErrorText=String][Path=String][AppID=String][ClusterID=String][NodeID=String]: ANN create local path error.

Explanation 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.

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.

Error Message

%UC_IPVMS-4-kIVRAudioCreateDirFailed: %[Error=ULong][ErrorText=String][Path=String][AppID=String][ClusterID=String][NodeID=String]: IVR create local path error

Explanation 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.

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.

Error Message

%UC_IPVMS-3-kANNAudioThreadWaitFailed: %[Error=ULong][AppID=String][ClusterID=String] [NodeID=String]: ANN TFTP event wait error.

Explanation An error was reported while waiting for a list of events. Announcement files will not be automatically updated.

Recommended Action Restart the Cisco IP Voice Media Streaming App service. If the error continues, restart the serverr.

Error Message

%UC_IPVMS-3-kANNAudioThreadException: %[ExceptionCode=ULong][AXReg=ULong] [BXReg=ULong][CXReg=ULong][DXReg=ULong][SIReg=ULong][DIReg=ULong][IPReg=ULong] [SPReg=ULong][BPReg=ULong][Flags=ULong][CSSeg=ULong][DSSeg=ULong][ESSeg=ULong] [SSSeg=ULong][FSSeg=ULong][GSSeg=ULong][AppID=String][ClusterID=String] [NodeID=String]: ANN TFTP transfer exception failure.

Explanation An unknown program exception has caused the background TFTP file transfer processing for announcement files to terminate. Announcement files will not be automatically updated.

Recommended Action Restart the Cisco IP Media Streaming App service and if the problem continues, report it to Cisco. Include CMS traces and Application Event log.

Error Message

%UC_IPVMS-3-kANNAudioThreadxFailed: %[Error=ULong][AppID=String][ClusterID=String] [NodeID=String]: ANN TFTP transfer thread creation failed.

Explanation The ANN background TFTP file transfer processing thread failed to create possibly due to low system resources.

Recommended Action Reboot server.

Error Message

%UC_IPVMS-3-kANNAudioComException: %[Filename=String][Reason=String][AppID=String] [ClusterID=String][NodeID=String]: ANN TFTP COM exception.

Explanation A COM exception occured while processing the specified file.

Recommended Action Review the file for possible format errors or missing elements.

Error Message

%UC_IPVMS-3-kANNAudioXmlLoadFailed: %[Filename=String][Reason=String][AppID=String] [ClusterID=String][NodeID=String]: ANN XML parsing error.

Explanation There is a syntax error in the specified file.

Recommended Action Correct the syntax error.

Error Message

%UC_IPVMS-3-kANNAudioXmlSyntax: %[Filename=String][AppID=String][ClusterID=String] [NodeID=String]: ANN XML invalid element .

Explanation There is an invalid element in the specified file.

Recommended Action Correct the error.

Error Message

%UC_IPVMS-3-kANNAudioTftpFileMissing: %[Filename=String][AppID=String][ClusterID=String] [NodeID=String]: ANN TFTP file missing.

Explanation A file was not found on the TFTP server to be downloaded to the announcement server.

Recommended Action Correct the error.

Error Message

%UC_IPVMS-3-kANNAudioTftpMgrStartFailed: %[FileName=String][AppID=String][ClusterID=String] [NodeID=String]: TFTP start file transfer failed.

Explanation Unable to start transfering a file from TFTP server.

Recommended Action Verify the file name exists on the TFTP server.

Error Message

%UC_IPVMS-3-kANNAudioTftpMgrCreate: %[TFTPServer=String][AppID=String][ClusterID=String] [NodeID=String]: Unable to create TFTP client.

Explanation Unable to create a client TFTP session with the TFTP server.. This may be due to the server not running, or an incorrect server name configuration setting in service paramenters. This operation will be retried periodically.

Recommended Action Verify the TFTP server is operating and configuration settings are correct.

Error Message

%UC_IPVMS-3-kANNAudioOpenFailed: %[Error=ULong][ErrorText=String][FileName=String] [AppID=String][ClusterID=String][NodeID=String]: Open announcement file failed.

Explanation An error was reported when attempting to open an announcement file for reading.

Recommended Action Verify the file exists and the Cisco IP Voice Media Streaming App service has proper access rights to open the file for reading.

Error Message

%UC_IPVMS-4-kANNAudioUndefinedLocale: %[LocaleID=ULong][Type=String][AppID=String] [ClusterID=String][NodeID=String]: Unknown ANN Locale.

Explanation 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.

Recommended Action Install the locale package or check device settings for an incorrect locale value.

Error Message

%UC_IPVMS-4-kIVRAudioUndefinedLocale: %[LocaleID=ULong][Type=String][AppID=String] [ClusterID=String][NodeID=String]: Unknown IVR Locale

Explanation 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.

Recommended Action Install the locale package or check device settings for an incorrect locale value.

Error Message

%UC_IPVMS-4-kANNAudioUndefinedAnnID: %[Locale=ULong][AnnID=ULong][AppID=String] [ClusterID=String][NodeID=String]: Requested announcement not found.

Explanation The requested announcement is unknown. This may be caused by using an incorrect announcement identifier for a custom announcement. Use the CUCM Admin to view a list of custom announcement identifiers and verify the correct one is being used.

Recommended Action Correct the announcement identifier chosen from the custom announcement list.

Error Message

%UC_IPVMS-4-kIVRAudioUndefinedIVRID: %[Locale=ULong][IVRID=ULong][AppID=String] [ClusterID=String][NodeID=String]: Requested announcement not found

Explanation The requested announcement is unknown. This may be caused by using an incorrect announcement identifier for a custom announcement. Use the CUCM Admin to view a list of custom announcement identifiers and verify the correct one is being used.

Recommended Action Correct the announcement identifier chosen from the custom announcement list.

Error Message

%UC_IPVMS-3-CFBDeviceRecoveryCreateFailed: %[Error=Int][ErrorText=String][AppID=String] [ClusterID=String][NodeID=String]: CFB device recovery create failure..

Explanation 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.

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

Error Message

%UC_IPVMS-3-UnableToOpenMohAudioSource: %[MohAudioSourceFileName=String] [MohAudioSourceId=UInt][Error=Int][ErrorText=String][AppID=String][ClusterID=String] [NodeID=String]: Music On Hold Audio Source file cannot be opened.

Explanation 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.

Recommended Action Use the CUCM Administration interface for "MOH Audio File Management" on this specific MOH CUCM 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 CUCM 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 it will be accessable by the MOH device.

Error Message

%UC_IPVMS-3-kCFBDeviceRecordNotFound: %[AppID=String][ClusterID=String] [NodeID=String]: CFB device record not found..

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

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

Error Message

%UC_IPVMS-4-kCFBDeviceStartingDefualts: %[Field=String][Value=String][AppID=String] [ClusterID=String][NodeID=String]: CFB device configuration not found..

Explanation 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.

Recommended Action Review the service parameter settings and configure the CFB device settings properly using the CUCM Administration.

Error Message

%UC_IPVMS-6-kCFBICMPErrorNotification: %[CID=ULong][PID=ULong][IP=String][Port=ULong] [AppID=String][ClusterID=String][NodeID=String]: CFB stream ICMP error..

Explanation 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.

Recommended Action No action is required. This may occur at times when connections are being stopped or redirected.

Error Message

%UC_IPVMS-4-kChangeNotifyServiceCreationFailed: %[Error=Int][ErrorText=String][AppID=String][ClusterID=String][NodeID=String]: Database change notification subsystem not starting..

Explanation 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.

Recommended Action Restart the Cisco IP Voice Media Streaming App service to get the DB notification reenabled.

Error Message

%UC_IPVMS-4-kChangeNotifyServiceGetEventFailed: %[Error=Int][ErrorText=String][AppID=String][ClusterID=String][NodeID=String]: Invalid notification event returned by database change notification..

Explanation 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.

Recommended Action Check the current status of the Cisco IP Voice Media Streaming App service and monitor for repeated occurances.

Error Message

%UC_IPVMS-4-kChangeNotifyServiceRestartFailed: %[Error=Int][ErrorText=String][AppID=String][ClusterID=String][NodeID=String]: Database change notification restart failure..

Explanation The change notification subsystem failed to restart.

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.

Error Message

%UC_IPVMS-3-kCreateAudioSourcesFailed: %[Error=Int][ErrorText=String][AppID=String][ClusterID=String][NodeID=String]: Creating audio source class failed..

Explanation Unable to create audio source subcombonent to provide audio for streaming. This may be due to lack of memory.

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

Error Message

%UC_IPVMS-3-kCreateControlFailed: %[AudioSourceID=ULong][CodecType=String][Error=Int][ErrorText=String][AppID=String][ClusterID=String][NodeID=String]: Stream Control create failure..

Explanation Create stream control subcomponent. The error may possibly be due to lack of memory.

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

Error Message

%UC_IPVMS-6-kReadCfgIpTosMediaResourceToCmNotFound: %[AppID=String][ClusterID=String][NodeID=String]: IP TOS MediaResource to Cm value not found..

Explanation 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).

Recommended Action Set the Ip Type-of-Service Media Resource To Call Manager service parameter for the Cisco IP Voice Media Streaming App service.

Error Message

%UC_IPVMS-4-kDeviceDriverError: %[Error=String][AppID=String][ClusterID=String] [NodeID=String]: IP voice media streaming device driver error..

Explanation The IP voice media streaming device driver returned an error. This may indicate a significant media error or resource shortage.

Recommended Action Restarting the Cisco IP Voice Media Streaming App service or possibly restarting the server may resolve the error condition.

Error Message

%UC_IPVMS-4-kDeviceMgrCreateFailed: %[DeviceName=String][ServerNumber=ULong] [ServerName=String][AppID=String][ClusterID=String][NodeID=String]: Device connection manager failed to start..

Explanation The device controller was unable to start a connection to control device registration with CallManager. This is possibly due to lack of memory.

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

Error Message

%UC_IPVMS-4-kDeviceMgrExitEventCreationFailed: %[DeviceName=String][TraceName=String] [Error=ULong][ErrorText=String][AppID=String][ClusterID=String][NodeID=String]: Creation of device manager exit event failed..

Explanation 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.

Recommended Action This error may be due to a memory resource shortage. Restart the Cisco IP Voice Media Streaming App service or restart the CUCM server.

Error Message

%UC_IPVMS-6-kDeviceMgrLockoutWithCallManager: %[TraceName=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco Unified Communications Manager in lockout..

Explanation The specified Cisco Unified Communications Manager has failed to respond to control messages. The TCP control connection to CUCM is being suspended. This will cause a switch to another CUCM 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 CUCM server.

Recommended Action Check the status of the Cisco Unified Communications Manager service. You may have to restart the CUCM service or the CUCM server.

Error Message

%UC_IPVMS-5-kDeviceMgrMoreThan50SocketEvents: %[TraceName=String][AppID=String] [ClusterID=String][NodeID=String]: More than 50 events returned from TCP link..

Explanation The specified Cisco Unified Communications Manager TCP link has returned a large number of TCP events. This indicates an unexpected flood of events.

Recommended Action No action is required. Monitor for reoccurance. This could be an indication of a security issue.

Error Message

%UC_IPVMS-4-kDeviceMgrOpenReceiveFailedOutOfStreams: %[TraceName=String][CID=ULong][PID=ULong][AppID=String][ClusterID=String][NodeID=String]: Open receive failure..

Explanation The open receive channel failed. This may indicate a missmatch of media resources between Cisco Unified Call Manager and the Cisco IP Voice Media Streaming App service.

Recommended Action Check the performance monitor counters for resource availability on CUCM 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 CUCM server.

Error Message

%UC_IPVMS-4-kDeviceMgrRegisterKeepAliveResponseError: %[TraceName=String][AppID=String][ClusterID=String][NodeID=String]: Cisco Unified Communications Manager not responding..

Explanation The specified Cisco Unified Communications Manager is not responding to the keepalive messages. The connection with CUCM 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 CUCM.

Recommended Action Cisco Unified Communications Manager may have gone down or is unable to respond. Check status of CUCM. The media device should automatically reregister.

Error Message

%UC_IPVMS-6-kDeviceMgrRegisterWithCallManager: %[TraceName=String][AppID=String][ClusterID=String][NodeID=String]: Registered with Cisco Unified Communications Manager..

Explanation The software media device registered with the specified Cisco Unified Communications Manager.

Recommended Action No action is required.

Error Message

%UC_IPVMS-4-kDeviceMgrRegisterWithCallManagerError: %[TraceName=String][AppID=String][ClusterID=String][NodeID=String]: Connection error with Cisco Unified Communications Manager..

Explanation 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.

Recommended Action No action is required. The media device will reregister.

Error Message

%UC_IPVMS-4-kDeviceMgrSocketDrvNotifyEvtCreateFailed: %[DeviceName=String][TraceName=String][Error=ULong][ErrorText=String][AppID=String][ClusterID=String][NodeID=String]: Create driver notification event failure..

Explanation An error was returned when creating a signaling event for communication with the media streaming kernel driver. This may be due to memory or system resource shortage.

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

Error Message

%UC_IPVMS-4-kDeviceMgrSocketNotifyEventCreateFailed: %[DeviceName=String] [TraceName=String][Error=ULong][ErrorText=String][AppID=String][ClusterID=String] [NodeID=String]: Creation socket event failure..

Explanation 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.

Recommended Action Restart the Cisco IP Voice Media Streaming App service and monitor for reoccurance or restart the CUCM server.

Error Message

%UC_IPVMS-4-kDeviceMgrStartTransmissionOutOfStreams: %[TraceName=String][CID=ULong] [PID=ULong][AppID=String][ClusterID=String][NodeID=String]: Start transmission failure..

Explanation An error was encountered while starting an RTP transmission audio stream. This may indicate a missmatch of resources between Cisco Unified Communications Manager and Cisco IP Voice Media Streaming App service.

Recommended Action Check the performance counters for the media resources on CUCM 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.

Error Message

%UC_IPVMS-6-kDeviceMgrThreadWaitFailed: %[TraceName=String][Error=Int][ErrorText=String] [AppID=String][ClusterID=String][NodeID=String]: Wait call failure in device manager thread..

Explanation An error was reported during a system request to wait on an event, the media device will be restarted.

Recommended Action No action is required.

Error Message

%UC_IPVMS-4-kDeviceMgrThreadxFailed: %[DeviceName=String][TraceName=String][Error=Int] [ErrorText=String][AppID=String][ClusterID=String][NodeID=String]: Creation of thread failure..

Explanation An error was reported when starting a process for the specified media device. This may be due to a system resource shortage.

Recommended Action Restart the Cisco IP Voice Media Streaming App service or restart the CUCM server to recover from this error.

Error Message

%UC_IPVMS-6-kDeviceMgrUnregisterWithCallManager: %[TraceName=String][AppID=String][ClusterID=String][NodeID=String]: Unregister with Cisco Unified Communications Manager..

Explanation A media device has unregistered with the specified Cisco Unified Communications Manager.

Recommended Action No action is required. The media device will automatically reregister.

Error Message

%UC_IPVMS-4-kFixedInputCreateControlFailed: %[AudioSourceID=ULong][CodecType=String][AppID=String][ClusterID=String][NodeID=String]: Fixed MOH stream control failed to start..

Explanation 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.

Recommended Action Reset MOH device, if failure continues restart the server. Monitor for errors in trace files and system log.

Error Message

%UC_IPVMS-4-kFixedInputCreateSoundCardFailed: %[AudioSourceID=ULong][CodecType=String][AppID=String][ClusterID=String][NodeID=String]: Fixed stream sound card interface failed to start..

Explanation 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.

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.

Error Message

%UC_IPVMS-4-kFixedInputInitSoundCardFailed: %[AudioSourceID=ULong][ErrorCode=ULong][ErrorCodeText=String][DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: Fixed stream sound card interface initialization failure..

Explanation Initialization of sound card failed. Fixed audio source will not play possibly due to missing or unconfigured USB sound device.

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 additionsl information.

Error Message

%UC_IPVMS-4-kFixedInputCodecStreamFailed: %[AudioSourceID=ULong][ErrorCode=ULong][ErrorCodeText=String][CodecType=String][AppID=String][ClusterID=String][NodeID=String]: Fixed input codec stream initialization failure..

Explanation Initialization of sound card codec source transcoding process failed. The fixed audio source will not play possibly due to memory or resource shortage.

Recommended Action Reset MOH device, or restart Cisco IO Voice Media Streaming App service, or restart server.

Error Message

%UC_IPVMS-4-kFixedInputTranscoderFailed: %[AudioSourceID=ULong][ErrorCode=ULong] [ErrorCodeText=String][AppID=String][ClusterID=String][NodeID=String]: Fixed input audio stream transcoder failure..

Explanation 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.

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.

Error Message

%UC_IPVMS-4-kGetFileNameFailed: %[AudioSourceID=ULong][CodecType=String][AppID=String] [ClusterID=String][NodeID=String]: Get audio source file name failure..

Explanation The Music-on-Hold audio source is not assigned to an audio file.

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.

Error Message

%UC_IPVMS-3-kIPVMSDeviceDriverNotFound: %[AppID=String][ClusterID=String] [NodeID=String]: Cisco IP voice media streaming driver not found..

Explanation 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.

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.

Error Message

%UC_IPVMS-4-kIPVMSMgrEventCreationFailed: %[Error=ULong][ErrorText=String][AppID=String] [ClusterID=String][NodeID=String]: Creation of required signaling event failed..

Explanation 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.

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.

Error Message

%UC_IPVMS-4-kIpVmsMgrThreadWaitFailed: %[AppID=String][ClusterID=String] [NodeID=String]: Error while waiting for asynchronous notifications of events..

Explanation 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).

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.

Error Message

%UC_IPVMS-3-kIpVmsMgrNoLocalHostName: %[AppID=String][ClusterID=String] [NodeID=String]: Unable to retrieve the local host server name..

Explanation Unable to obtain 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.

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.

Error Message

%UC_IPVMS-3-kIpVmsMgrNoLocalNetworkIPAddr: %[AppID=String][ClusterID=String] [NodeID=String]: Unable to retrieve the network IP address for host server..

Explanation 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.

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).

Error Message

%UC_IPVMS-4-kIPVMSMgrThreadxFailed: %[Error=ULong][ErrorText=String][AppID=String] [ClusterID=String][NodeID=String]: Creation of the IPVMSMgr thread failed..

Explanation 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.

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.

Error Message

%UC_IPVMS-3-kIPVMSMgrWrongDriverVersion: %[Found=ULong][Need=ULong][AppID=String] [ClusterID=String][NodeID=String]: Wrong version of device driver..

Explanation 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.

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.

Error Message

%UC_IPVMS-6-kIPVMSStarting: %[Version=String][IPAddress=String][Hostname=String] [ServiceName=String][ProcessID=ULong][AppID=String][ClusterID=String][NodeID=String]: IP voice media streaming application starting..

Explanation The Cisco IP Voice Media Streaming App service is starting.

Recommended Action No action is required.

Error Message

%UC_IPVMS-6-kIPVMSStopping: %[Version=String][IPAddress=String][Hostname=String] [ServiceName=String][ProcessID=ULong][AppID=String][ClusterID=String][NodeID=String]: The IP voice media streaming application shutting down..

Explanation The Cisco IP Voice Media Streaming App service is shutting down.

Recommended Action No action is required.

Error Message

%UC_IPVMS-4-kMOHBadMulticastIP: %[AudioSourceID=ULong][ConferenceID=ULong] [CodecType=String][IPAddress=String][Port=ULong][AppID=String][ClusterID=String] [NodeID=String]: Invalid multicast IP address..

Explanation An invalid multicast IP address (out of range) was found.

Recommended Action Correct the setting on the Music-on-Hold device configuration for multicast address.

Error Message

%UC_IPVMS-4-kMOHDeviceRecordNotFound: %[AppID=String][ClusterID=String] [NodeID=String]: MOH device record not found..

Explanation A Music-on-Hold device was not found for this server. This device is normally automatically added when a server is added to the configuration.

Recommended Action If Music-on-Hold functionality is required, you will need to remove and readd server to the database. WARNING: This may impact many other configuration settings (CM Groups, Media Resource Groups, etc...).

Error Message

%UC_IPVMS-6-kMOHICMPErrorNotification: %[CID=ULong][PID=ULong][IP=String][Port=ULong] [AppID=String][ClusterID=String][NodeID=String]: MOH stream ICMP error..

Explanation 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.

Recommended Action No action is required.

Error Message

%UC_IPVMS-4-kMOHMgrCreateFailed: %[Error=ULong][ErrorText=String][AppID=String] [ClusterID=String][NodeID=String]: Error starting MOH Audio source subcomponent..

Explanation 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).

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

Error Message

%UC_IPVMS-4-kMOHMgrExitEventCreationFailed: %[Error=ULong][ErrorText=String][AppID=String] [ClusterID=String][NodeID=String]: Creation of MOH manager exit event failed..

Explanation An error was encountered when allocating a signaling event. This may be caused by a resource shortage.

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

Error Message

%UC_IPVMS-6-kMOHMgrIsAudioSourceInUseThisIsNULL: %[AppID=String][ClusterID=String] [NodeID=String]: Synchronization error detected in MOH audio manager..

Explanation A synchronization error was detected. Condition has been resolved automatically.

Recommended Action No action is required.

Error Message

%UC_IPVMS-6-kMOHMgrThreadWaitFailed: %[Error=ULong][ErrorText=String][AppID=String] [ClusterID=String][NodeID=String]: Wait call failure in MOH manager thread..

Explanation An error was encountered in Music-on-Hold audio manager subcomponent while waiting for aynchronous event signaling. The MOH device will be restarted.

Recommended Action No action is required.

Error Message

%UC_IPVMS-4-kMOHMgrThreadxFailed: %[Error=ULong][ErrorText=String][AppID=String] [ClusterID=String][NodeID=String]: Starting of MOH audio manager failed..

Explanation An error was encountered when starting the Music-on-Hold audio manager subcomponent. Music-on-Hold audio services will not be avaliable.

Recommended Action Restart the Cisco IP Voice Media Streaming App service.

Error Message

%UC_IPVMS-6-kMOHRewindStreamControlNull: %[AudioSourceID=ULong][CodecType=String]

[AppID=String][ClusterID=String][NodeID=String]: Attempted to rewind an inactive MOH audio source..

Explanation An attempt was made to rewind or restart the Music-on-Hold audio source that is inactive. This has been ignored.

Recommended Action No action required.

Error Message

%UC_IPVMS-6-kMOHRewindStreamMediaPositionObjectNull: %[AudioSourceID=ULong] [CodecType=String][AppID=String][ClusterID=String][NodeID=String]: Error rewinding MOH audio source that is not playing..

Explanation An attempt was made to rewind or restart a Music-on-Hold wav file that was not being played. This has been ignored.

Recommended Action No action is required.

Error Message

%UC_IPVMS-3-kMOHTFTPGoRequestFailed: %[ErrorText=String][File=String][SrcPath=String] [DstPath=String][OSError=Int][OSErrorText=String][AppID=String][ClusterID=String] [NodeID=String]: Transfer of MOH source file to working path failed..

Explanation An error was encountered when trying to copy or update a Music-on-Hold audio source file.

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

Error Message

%UC_IPVMS-4-kMTPDeviceRecordNotFound: %[AppID=String][ClusterID=String] [NodeID=String]: MTP device record not found..

Explanation 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.

Recommended Action If MTP functionality is required, you will need to delete the server and re-add the server back to the database using CCMAdmin. WARNING: This may require many additional configuration settings to be reapplied such as CallManager Groups, Media Resource groups and more.

Error Message

%UC_IPVMS-6-kMTPDeviceStartingDefualts: %[CallCount=ULong][RunFlag=String][AppID=String][ClusterID=String][NodeID=String]: MTP device configuration not found, starting with defaults..

Explanation 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.

Recommended Action Configure the service parameter settings for the MTP device.

Error Message

%UC_IPVMS-3-kReadCfgCFBComException: %[DeviceName=String][Description=String][AppID=String][ClusterID=String][NodeID=String]: COM error..

Explanation A COM error occurred while trying to read CFB configuration information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgCFBDblException: %[DeviceName=String][ExceptionStr=String][ExceptionID=ULong][AppID=String][ClusterID=String][NodeID=String]: Database exception..

Explanation A database exception occurred while trying to read CFB configuration information.

Recommended Action Device will not start; fix database problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgCFBListComException: %[DeviceName=String][Description=String][AppID=String][ClusterID=String][NodeID=String]: COM error..

Explanation A COM error occurred while trying to read CFB Cisco Unified Communications Manager list information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgCFBListDblException: %[DeviceName=String][ExceptionStr=String][ExceptionID=ULong][AppID=String][ClusterID=String][NodeID=String]: Database exception..

Explanation A database exception occurred while trying to read CFB Cisco Unified Communications Manager list information.

Recommended Action Device will not start; fix database problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgCFBListUnknownException: %[DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: Unknown exception..

Explanation An unknown exception occurred while trying to read CFB Cisco Unified Communications Manager list information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgCFBUnknownException: %[DeviceName=String][AppID=String]

[ClusterID=String][NodeID=String]: Unknown exception..

Explanation An unknown exception occurred while trying to read CFB configuration information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-6-kReadCfgDblGetChgNotifyFailed: %[AppID=String][ClusterID=String] [NodeID=String]: Get change notification port failure..

Explanation The database layer was unable to find change notification port and is using default.

Recommended Action If default change notification is incorrect or change notification does not work, add value into database and restart service.

Error Message

%UC_IPVMS-3-kReadCfgDblGetNodeNameFailed: %[AppID=String][ClusterID=String] [NodeID=String]: Database layer select my process node failed..

Explanation The database layer was unable to find/determine the current node on which this service is running.

Recommended Action Make sure the database is configured properly.

Error Message

%UC_IPVMS-3-kReadCfgMOHAudioSourceComException: %[DeviceName=String] [Description=String][AppID=String][ClusterID=String][NodeID=String]: COM error..

Explanation A COM error occurred while trying to read MOH audio sources.

Recommended Action Audio sources will be disabled; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMOHAudioSourceDblException: %[DeviceName=String] [ExceptionStr=String][ExceptionID=ULong][AppID=String][ClusterID=String] [NodeID=String]: Database exception..

Explanation A database exception occurred while trying to read MOH audio sources.

Recommended Action Audio sources will be disabled; fix database problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMOHAudioSourceUnknownException: %[DeviceName=String] [AppID=String][ClusterID=String][NodeID=String]: Unknown exception..

Explanation An unknown exception occurred while trying to read MOH audio sources.

Recommended Action Audio sources will be disabled; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMOHComException: %[DeviceName=String][Description=String] [AppID=String][ClusterID=String][NodeID=String]: COM error..

Explanation A COM error occurred while trying to read MOH configuration information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMOHDblException: %[DeviceName=String][ExceptionStr=String] [ExceptionID=ULong][AppID=String][ClusterID=String][NodeID=String]: Database exception..

Explanation A database exception occurred while trying to read MOH configuration information.

Recommended Action Device will not start; fix database problem and restart service.

Error Message

%UC_IPVMS-6-kReadCfgMOHEnabledCodecsNotFound: %[AppID=String][ClusterID=String] [NodeID=String]: MOH enabled codecs not found..

Explanation The Music-on-Hold service parameter for codec selection could not be read from database. Defaulting to G.711 mu-law codec.

Recommended Action Set the Music-on-Hold service parameter for Cisco IP Voice Media Streaming

App service.

Error Message

%UC_IPVMS-3-kReadCfgEnterpriseComException: %[Description=String][AppID=String] [ClusterID=String][NodeID=String]: COM error..

Explanation A COM error occurred while trying to read clsterwide service parameters.

Recommended Action MOH or ANN audio sources may be unavailable; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgEnterpriseDblException: %[ExceptionStr=String][ExceptionID=ULong] [AppID=String][ClusterID=String][NodeID=String]: Database exception..

Explanation A database exception occurred while trying to read clusterwide service parameters.

Recommended Action MOH or ANN audio sources may be unavailable; fix database problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgEnterpriseUnknownException: %[AppID=String][ClusterID=String] [NodeID=String]: Unknown exception..

Explanation An unknown exception occurred while tring to read clusterwide service parameters.

Recommended Action MOH or ANN audio sources may be unavailable; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMOHListComException: %[DeviceName=String][Description=String] [AppID=String][ClusterID=String][NodeID=String]: COM error..

Explanation A COM error occurred while trying to read MOH Cisco Unified Communications Manager list information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMOHListDblException: %[DeviceName=String][ExceptionStr=String] [ExceptionID=ULong][AppID=String][ClusterID=String][NodeID=String]: Database exception..

Explanation A database exception occurred while trying to read MOH Cisco Unified Communications Manager list information.

Recommended Action Device will not start; fix database problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMOHListUnknownException: %[DeviceName=String][AppID=String] [ClusterID=String][NodeID=String]: Unknown exception..

Explanation An unknown exception occurred while trying to read MOH Cisco Unified Communications Manager list information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMOHServerComException: %[DeviceName=String][Description=String] [AppID=String][ClusterID=String][NodeID=String]: COM error..

Explanation A COM error occurred while trying to read MOH device information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMOHServerDblException: %[DeviceName=String][ExceptionStr=String] [ExceptionID=ULong][AppID=String][ClusterID=String][NodeID=String]: Database exception..

Explanation A database exception occurred while trying to read MOH device information.

Recommended Action Device will not start; fix database problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMOHServerUnknownException: %[DeviceName=String][AppID=String] [ClusterID=String][NodeID=String]: Unknown exception..

Explanation An unknown exception occurred while trying to read MOH device information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMOHTFTIPAddressNotFound: %[AppID=String][ClusterID=String] [NodeID=String]: MOH TFTP IP address not found..

Explanation The default MOH TFTP IP address was not found in the database.

Recommended Action Audio sources may be unavailable; create proper value in database and

restart service.

Error Message

%UC_IPVMS-3-kReadCfgMOHUnknownException: %[DeviceName=String][AppID=String] [ClusterID=String][NodeID=String]: Unknown exception..

Explanation An unknown exception occurred while trying to read MOH configuration information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMTPComException: %[DeviceName=String][Description=String] [AppID=String][ClusterID=String][NodeID=String]: COM error..

Explanation A COM error occurred while trying to read MTP configuration information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMTPDblException: %[DeviceName=String][ExceptionStr=String] [ExceptionID=ULong][AppID=String][ClusterID=String][NodeID=String]: Database exception..

Explanation A database exception occurred while trying to read MTP configuration information.

Recommended Action Device will not start; fix database problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMTPListComException: %[DeviceName=String][Description=String] [AppID=String][ClusterID=String][NodeID=String]: COM error..

Explanation A COM error occurred while trying to read MTP Cisco Unified Communications Manager list information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMTPListDblException: %[DeviceName=String][ExceptionStr=String] [ExceptionID=ULong][AppID=String][ClusterID=String][NodeID=String]: Database exception..

Explanation A database exception occurred while trying to read MTP Cisco Unified Communications Manager list information.

Recommended Action Device will not start; fix database problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMTPListUnknownException: %[DeviceName=String][AppID=String] [ClusterID=String][NodeID=String]: Unknown exception..

Explanation An unknown exception occurred while trying to read MTP Cisco Unified Communications Manager list information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-3-kReadCfgMTPUnknownException: %[DeviceName=String][AppID=String]

[ClusterID=String][NodeID=String]: Unknown exception..

Explanation An unknown exception occurred while trying to read MTP configuration information.

Recommended Action Device will not start; fix problem and restart service.

Error Message

%UC_IPVMS-4-kRequestedCFBStreamsFailed: %[Requested=ULong][Allocated=ULong] [AppID=String][ClusterID=String][NodeID=String]: CFB requested streams failure..

Explanation The resources for the number of requested full-duplex streams was not available.

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.

Error Message

%UC_IPVMS-4-kRequestedMOHStreamsFailed: %[Requested=ULong][Allocated=ULong] [AppID=String][ClusterID=String][NodeID=String]: MOH requested streams failure..

Explanation The resources for the number of requested streams was not available.

Recommended Action Verify the number of calls configuration setting for Music-on-Hold device. Restart the server to reset the resources.

Error Message

%UC_IPVMS-4-kRequestedMTPStreamsFailed: %[Requested=ULong][Allocated=ULong] [AppID=String][ClusterID=String][NodeID=String]: MTP requested streams failure..

Explanation The resources for the number of requested full-duplex Media Termination Point streams was not available.

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.

Error Message

%UC_IPVMS-4-MOHDeviceRecoveryCreateFailed: %[Error=ULong][ErrorText=String][AppID=String] [ClusterID=String][NodeID=String]: MOH device recovery create failure..

Explanation An error was encountered restarting the Music-on-Hold device. This may be caused by a shortage of memory resources.

Recommended Action Check the status of the Music-on-Hold device. If the MOH device is not registered and available, Restart the Cisco IP Voice Media Streaming App service or restart the server.

Error Message

%UC_IPVMS-4-MTPDeviceRecoveryCreateFailed: %[Error=ULong][ErrorText=String][AppID=String][ClusterID=String][NodeID=String]: MTP device recovery create failure..

Explanation An error was encountered trying to restart the Media Termination Point device. This may be due to a shortage of application memory.

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

Error Message

%UC_IPVMS-4-SoftwareLicenseNotValid: %[AppID=String][ClusterID=String][NodeID=String]: Invalid Software License..

Explanation There is no valid software license; the Cisco IP Voice Media Streaming App service requires a valid software license to operate.

Recommended Action Install a valid software license and restart Cisco IP Voice Media Streaming App service.

Error Message

%UC_IPVMS-6-SoftwareLicenseValid: %[AppID=String][ClusterID=String][NodeID=String]: Valid Software License Found..

Explanation A valid software license has been detected by the IP Voice Media Streaming App service.

Recommended Action No action required. This informational message indicates alarm SoftwareLicenseNotValid is cleared.

Error Message

%UC_IPVMS-4-kANNAudioFileMissing: %[Filename=String][AnnouncementID=ULong][UserLocale=ULong][NetworkLocale=ULong][AppID=String][ClusterID=String][NodeID=String]: Announcement file not found..

Explanation 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.

Recommended Action Upload the custom announcement to the server or install the missing locale package.

Error Message

%UC_IPVMS-3-CryptoCapabilityFailed: %[Devicename=String][AppID=String][ClusterID=String][NodeID=String]: Failed to initialize sRTP crypto..

Explanation The media device shown in this alarm attempted to load and initialize crypto capabilities within the operating system kernel, however, a failure, such as the OS lacking encryption configuration, a memory shortage, or crypto self-test failure, occurred during initialization. Secure media encryption for this device has been disabled as a result, but unencrypted media is still supported. All media streams are non-secure (unencrypted) for this device. This alarm is capable of occurring when the crypto failure occurs because the Cisco IP Voice Media Streaming App service parameter Force Annunciator to be Non-secure or Force MOH to be Non-secure is enabled.

Recommended Action Use the Cisco Unified Real-Time Monitoring Tool (RTMT) to retrieve the system log. Review the system log and respond to error messages containing sRTP or IpVms.

Error Message

%UC_IPVMS-4-PlayAnnouncementFailure: %[ReasonCode=ULong][Identifier=String][Locale=String][AnnouncementEnum=ULong][FileName=String][CustomFileName=String][AppID=String][ClusterID=String][NodeID=String]: Unable to play a requested announcement or tone.

Explanation Reason code explanations: [1] Announcement requested is undefined. The announcement enum number is unknown. [2] Locale requested is unknown. The requested locale has not been installed on this node. [3] The customized announcement file does not exist on this server node for the locale. If a default system announcement is assigned, it will be used in place of the customized announcement. [4] Internal annunciator resource shortage has caused the announcement to fail. [5] System announcement or tone file not found.

Recommended Action Recommendations based on reason code: [1] this is usually a system design issue and cannot be resolved by normal means; [2] Be sure the requested locale is installed on each CUCM server node; [3] Upload the customized announcement wav file to this server node using CCM Administration on this node; [4] Review the annunciator device configuration for maximum number of calls and/or schedule an annunciator device reset as a temporary workaround to ensure orphanned resources are released or restart the Cisco IP Voice Media Streaming App service; [5] Check locale is installed on CUCM server node or possible missing file not installed properly.

Error Message

%UC_TFTP-1-CreateThreadFailed: %[Error=Int][Reason=String][AppID=String][ClusterID=String][NodeID=String]: Failed to create a new thread. See Reason string for where it failed..

Explanation This usually happens when there are system issues such as running out of memory resources.

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.

Error Message

%UC_TFTP-1-SDIControlLayerFailed: %[Error=Int][Reason=String][AppID=String][ClusterID=String][NodeID=String]: Failed to update trace logging or alarm subsystem for new settings..

Explanation This usually indicates a lack of system resources or a failure in database access by the trace logging or alarm subsystem.

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 error messages 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.

Error Message

%UC_TFTP-3-ConfigThreadReadConfigurationFailed: %[AppID=String][ClusterID=String][NodeID=String]: Failed to retrieve enterprise parameter values from database at TFTP service startup..

Explanation This is usually caused by database access failure.

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 error messages that may have occurred around the time of the alarm.

Error Message

%UC_TFTP-3-ConfigThreadBuildFileFailed: %[AppID=String][ClusterID=String][NodeID=String]: Failed to build all device configuration files at TFTP service startup..

Explanation This is usually caused by database access failure.

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 error messages that may have occurred around the time of the alarm.

Error Message

%UC_TFTP-1-ConfigThreadChangeNotifyServerInstanceFailed: %[AppID=String][ClusterID=String][NodeID=String]: Failed to allocate resources to handle configuration change notification from database..

Explanation This usually indicates a lack of memory when there is a system issue such as running out of resources.

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.

Error Message

%UC_TFTP-1-ConfigThreadChangeNotifyServerSingleFailed: %[AppID=String][ClusterID=String][NodeID=String]: Failed to allocate resources to handle configuration change notification from database..

Explanation This usually indicates a lack of memory when there is a system issue such as running out of resources.

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.

Error Message

%UC_TFTP-1-ConfigThreadChangeNotifyServerStartFailed: %[AppID=String][ClusterID=String][NodeID=String]: Failed to start listening to configuration change notification from database..

Explanation This usually indicates a lack of memory when there is a system issue such as running out of resources.

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.

Error Message

%UC_TFTP-3-ConfigThreadCNCMGrpBuildFileFailed: %[AppID=String][ClusterID=String][NodeID=String]: Failed to rebuild configuration files for changes in Cisco Unified Communications Manager Group settings..

Explanation This is usually caused by a failure to access the Cisco Unified Communications Manager database.

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 error messages that may have occurred around the time of the alarm.

Error Message

%UC_TFTP-3-ConfigThreadCNGrpBuildFileFailed: %[AppID=String][ClusterID=String] [NodeID=String]: Failed to rebuild configuration files for changes at group level settings such as Device Pool or Common Device Config settings..

Explanation This is usually caused by a failure to access the Cisco Unified Communications Manager database.

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 error messages that may have occurred around the time of the alarm.

Error Message

%UC_TFTP-3-ConfigThreadUnknownExceptionCaught: %[AppID=String][ClusterID=String] [NodeID=String]: An exception is caught in the main processing routine..

Explanation 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.

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

Error Message

%UC_TFTP-3-ReadConfigurationUnknownException: %[AppID=String][ClusterID=String] [NodeID=String]: An exception is caught while retrieving enterprise parameters value from database at TFTP service startup..

Explanation This is usually caused by a failure to access the Cisco Unified Communications Manager database.

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 error messages that may have occurred around the time of the alarm.

Error Message

%UC_TFTP-3-ConfigItAllReadConfigurationFailed: %[AppID=String][ClusterID=String] [NodeID=String]: Failed to retrieve enterprise parameter values from database when rebuilding all configuration files..

Explanation This is usually caused by a failure to access the Cisco Unified Communications Manager database.

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 error messages that may have occurred around the time of the alarm.

Error Message

%UC_TFTP-3-ConfigItAllBuildFilesFailed: %[AppID=String][ClusterID=String][NodeID=String]: A complete rebuild of all device configuration files has failed..

Explanation Probable causes of this alarm could be failure to access the Cisco Unified Communications Manager database, or misconfiguration of some devices.

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 error messages that may have occurred around the time of the alarm.

Error Message

%UC_TFTP-1-SocketError: %[nError=Int][Reason=String][AppID=String][ClusterID=String][NodeID=String]: Failed to open network connection for receiving file requests..

Explanation This usually happens when the IP address that the TFTP service uses to open the network connection is invalid.

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).

Error Message

%UC_TFTP-1-TFTPServerListenSetSockOptFailed: %[nError=Int][IPAddress=String][Port=Int][AppID=String][ClusterID=String][NodeID=String]: Failed to increase the size of the network buffer for receiving file requests..

Explanation This usually indicates a lack of memory when there is a system issue such as running out of resources.

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.

Error Message

%UC_TFTP-1-TFTPServerListenBindFailed: %[nError=Int][IPAddress=String][Port=Int][AppID=String][ClusterID=String][NodeID=String]: Fail to connect to the network port through which file requests are received..

Explanation 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.

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).

Error Message

%UC_TFTP-4-NoCallManagerFound: %[Error=String][AppID=String][ClusterID=String] [NodeID=String]: No Cisco Unified Communications Manager (Unified CM, formerly known as Cisco Unified CallManager) node has been configured..

Explanation A Cisco Unified Communications Manager Group exists but it has no Unified CM node configured as its group member.

Recommended Action In Cisco Unified CM Administration (System > Cisco Unified CM Group), configure at least one Unified CM node for the Unified CM Group referenced in this alarm. The Unified CM Group is part of the device pool to which the specified phone belongs.

Error Message

%UC_TFTP-3-CNFFBuffWriteToFilefopenfailed: %[FileName=String][AppID=String][ClusterID=String] [NodeID=String]: Failed to create Config File on disk or update existing Config File on disk..

Explanation This may happen if disk is full or the file is in use.

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).

Error Message

%UC_TFTP-3-CNFFBuffWriteToFilefwritefailed: %[FileName=String][AppID=String][ClusterID=String] [NodeID=String]: Failed to save Config File to disk..

Explanation This may happen if disk is full or the file is in use.

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).

Error Message

%UC_TFTP-4-ServingFileWarning: %[ErrorNumber=Int][FileName=String][IPAddress_Port=String] [Mode=String][OpCode=Int][Reason=String][AppID=String][ClusterID=String][NodeID=String]: There was an error during processing of file request..

Explanation 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.

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 (Unified CM). Either add the phone to 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).

Error Message

%UC_TFTP-3-ThreadPoolProxyUnknownException: %[AppID=String][ClusterID=String] [NodeID=String]: Unknown exception was caught while processing file request..

Explanation This usually indicates a lack of memory when there is a system issue such as running out of resources.

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.

Error Message

%UC_TFTP-6-BuildStat: %[DeviceCount=Int][DeviceTime=Int][UnitCount=Int][UnitTime=Int] [SoftkeyCount=Int][SoftkeyTime=Int][FeatureControlPolicyTime=Int][FeatureControlPolicyCount=Int] [DialruleCount=Int][DialruleTime=Int][TotalTime=Int][BuildStatus=String][AppID=String] [ClusterID=String][NodeID=String]: Device configuration files are being built..

Explanation This alarm provides information about the BUILD ALL operation to build all types of configuration files.

Recommended Action This alarm is for information purposes only; no action is required.

Error Message

%UC_TFTP-3-IPv6InterfaceNotInstalled: %[AppID=String][ClusterID=String][NodeID=String]: IPv6 network interface is not installed..

Explanation 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.

Recommended Action Install IPv6 network interface and then restart TFTP service.

Error Message

%UC_TFTP-5-ITLFileRegenerated: %[AppID=String][ClusterID=String][NodeID=String]: ITL file regeneration.

Explanation This is for regeneration of ITLFile

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.

Error Message

%UC_TFTP-1-OFFClusternodedown: %[IpAddress=String][AppID=String][ClusterID=String] [NodeID=String]: OFFCluster node is down

Explanation This is to indicate that the offcluster node is down.

Recommended Action Proxy-offcluster configuration is enabled and this node is configured as an offcluster-node.Please ensure that TFTP service on offcluster node is up and running for the proxy-offcluster configuration to work properly.If it is not an intended configuration please uncheck the TFTP check box in cluster view configuration in UI.

Error Message

%UC_TCD-0-IPAddressResolveError: %[HostName=String][AppID=String][ClusterID=String] [NodeID=String]: The IP Address for host was NOT RESOLVED.

Explanation The IP Address for host was NOT RESOLVED

Recommended Action NONE

Error Message

%UC_TCD-0-NoCMEntriesInDB: %[AppID=String][ClusterID=String][NodeID=String]: There are no CallManager entries in the database..

Explanation There are no CallManager entries in the database.

Recommended Action NONE

Error Message

%UC_TCD-6-LoadShareDeActivateTimeout: %[AppID=String][ClusterID=String] [NodeID=String]: There was timeout during wait for DeActivateLoadShare acknowledgement.

Explanation There was timeout during wait for DeActivateLoadShare acknowledgement

Recommended Action NONE

Error Message

%UC_TCD-0-LineStateSrvEngCreationError: %[AppID=String][ClusterID=String] [NodeID=String]: There was an error during the LineStateSrvEng Creation.

Explanation There was an error during the LineStateSrvEng Creation

Recommended Action NONE

Error Message

%UC_TCD-0-GlobalSPUtilsCreationError: %[AppID=String][ClusterID=String][NodeID=String]: There was an error during the GlobalSPUtils creation.

Explanation There was an error during the GlobalSPUtils creation

Recommended Action NONE

Error Message

%UC_TCD-0-TapiLinesTableCreationError: %[AppID=String][ClusterID=String][NodeID=String]: There was an error during the TapiLinesTable creation.

Explanation There was an error during the TapiLinesTable creation

Recommended Action NONE

Error Message

%UC_TCD-0-HuntGroupControllerCreationError: %[AppID=String][ClusterID=String] [NodeID=String]: There was an error during the HuntGroupController creation.

Explanation There was an error during the HuntGroupController creation

Recommended Action NONE

Error Message

%UC_TCD-0-HuntGroupCreationError: %[AppID=String][ClusterID=String][NodeID=String]: There was

an error during the Hunt Group creation.

Explanation There was an error during the Hunt Group creation

Recommended Action NONE

Error Message

%UC_TCD-0-CallDirectorCreationError: %[AppID=String][ClusterID=String][NodeID=String]: There was an error during the CallDirector creation.

Explanation There was an error during the CallDirector creation

Recommended Action NONE

Error Message

%UC_TCD-0-SysControllerCreationError: %[AppID=String][ClusterID=String][NodeID=String]: There was an error during the SysController creation.

Explanation There was an error during the SysController creation

Recommended Action NONE

Error Message

%UC_TCD-0-TimerServicesCreationError: %[AppID=String][ClusterID=String][NodeID=String]: There was an error during the TimerServices creation.

Explanation There was an error during the TimerServices creation

Recommended Action NONE

Error Message

%UC_TCD-3-DBLGetVersionInfoError: %[AppID=String][ClusterID=String][NodeID=String]: DBL GetVersionInfo function returned NULL.

Explanation DBL GetVersionInfo function returned NULL

Recommended Action NONE

Error Message

%UC_TCD-0-ExcceptionInInitSDIConfiguration: %[AppID=String][ClusterID=String] [NodeID=String]: Exception occured in InitSDIConfiguration function.

Explanation Exception occured in InitSDIConfiguration function

Recommended Action NONE

Error Message

%UC_TCD-0-SyncDBCreationError: %[AppID=String][ClusterID=String][NodeID=String]: There was an error during the SyncDB creation in SysController.

Explanation There was an error during the SyncDB creation in SysController

Recommended Action NONE

Error Message

%UC_TCD-0-LostConnectionToCM: %[AppID=String][ClusterID=String][NodeID=String]: Connection

to CallManager was lost.

Explanation Connection to CallManager was lost

Recommended Action NONE

Error Message

%UC_TCD-6-UserLoginSuccess: %[UserID=String][AppID=String][ClusterID=String] [NodeID=String]: User successfully logged in..

Explanation User successfully logged in.

Recommended Action NONE

Error Message

%UC_TCD-3-UserLoginFailed: %[UserID=String][AppID=String][ClusterID=String] [NodeID=String]: User log in failed because of bad user id or password..

Explanation User log in failed because of bad user id or password.

Recommended Action NONE

Error Message

%UC_TCD-6-UserAlreadyLoggedIn: %[UserID=String][AppID=String][ClusterID=String] [NodeID=String]: User is already logged in.

Explanation User is already logged in

Recommended Action NONE

Error Message

%UC_TCD-6-UserLoggedOut: %[UserID=String][AppID=String][ClusterID=String] [NodeID=String]: User logged out.

Explanation User logged out

Recommended Action NONE

Error Message

%UC_TCD-6-AgentOnline: %[AppID=String][ClusterID=String][NodeID=String]: Agent online.

Explanation Agent online

Recommended Action NONE

Error Message

%UC_TCD-6-AgentOffline: %[AppID=String][ClusterID=String][NodeID=String]: Agent offline.

Explanation Agent offline

Recommended Action NONE

Error Message

%UC_DirSync-6-CiscoDirSyncStarted: %[AppID=String][ClusterID=String][NodeID=String]: Cisco DirSync Application started .

Explanation Application started successfully

Recommended Action No action required.

Error Message

%UC_DirSync-0-CiscoDirSyncStartFailure: %[AppID=String][ClusterID=String][NodeID=String]: Cisco DirSymc application failed to start successfully.

Explanation Error occurred while starting application

Recommended Action See application logs for error, may require restarting the application

Error Message

%UC_DirSync-6-CiscoDirSyncProcessStarted: %[AgreementId=String][AppID=String] [ClusterID=String][NodeID=String]: LDAPSync process started on particular sync agreement.

Explanation LDAPSync process started to sync user data on the configured agreement id

Recommended Action No action required

Error Message

%UC_DirSync-2-CiscoDirSyncProcessFailToStart: %[AgreementId=String][AppID=String] [ClusterID=String][NodeID=String]: LDAPSync process failed to start on particular sync agreement.

Explanation LDAPSync process failed to start on the configured agreement id

Recommended Action See application logs for error

Error Message

%UC_DirSync-6-CiscoDirSyncProcessCompleted: %[AgreementId=String][AppID=String] [ClusterID=String][NodeID=String]: LDAPSync process completed on particular sync agreement.

Explanation LDAPSync process completed to sync user data on the configured agreement id

Recommended Action No action required

Error Message

%UC_DirSync-6-CiscoDirSyncProcessStoppedManually: %[AgreementId=String][AppID=String] [ClusterID=String][NodeID=String]: LDAPSync process stopped manually on particular sync agreement.

Explanation LDAPSync process stopped manually on the configured agreement id

Recommended Action No action required

Error Message

%UC_DirSync-6-CiscoDirSyncProcessStoppedAuto: %[AgreementId=String][AppID=String] [ClusterID=String][NodeID=String]: LDAPSync process stopped automatically on particular sync agreement.

Explanation LDAPSync process stopped automatically on the configured agreement id, it will be restarted automatically

Recommended Action No action required

Error Message

%UC_DirSync-3-CiscoDirSyncProcessFailedRetry: %[AgreementId=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: LDAPSync process failed on particular sync agreement.

Explanation LDAPSync process failed to sync user data on the configured agreement id

Recommended Action No action required. The sync process will automatic retry See application logs

for details

Error Message

%UC_DirSync-3-CiscoDirSyncProcessFailedNoRetry: %[AgreementId=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: LDAPSync process failed on particular sync agreement.

Explanation LDAPSync process failed to sync user data on the configured agreement id

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

Error Message

%UC_DirSync-3-CiscoDirSyncProcessConnectionFailed: %[AgreementId=String][LDAPHost=String] [Reason=String][AppID=String][ClusterID=String][NodeID=String]: LDAPSync process failed to connect to LDAP server.

Explanation LDAPSync process failed to connect to LDAP host

Recommended Action Please make sure 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

Error Message

%UC_DirSync-3-CiscoDirSyncDBAccessFailure: %[AgreementId=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: LDAPSync process failed to access local database.

Explanation CiscoDirSync failed to access local database

Recommended Action Please make sure the local CallManager database is working properly. The failed sync process will restart at the next scheduled time.

Error Message

%UC_DirSync-6-CiscoDirsyncZeroUsersSynced: %[AgreementId=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: LDAPSync process synced zero users for the sync agreement.

Explanation CiscoDirSync synced zero users

Recommended Action Check the application logs for details

Error Message

%UC_DirSync-6-UserUpdated: %[AgreementId=String][Userid=String][Reason=String][AppID=String] [ClusterID=String][NodeID=String]: LDAPSync process found a user with the same userid synced from a different LDAP agreement. Updated the already existing user in the DB with the new user synced .

Explanation LDAPSync process found a user with the same userid synced from a different LDAP agreement. Updated the already existing user in the DB with the new user synced

Recommended Action No action required

Error Message

%UC_DirSync-4-DirSyncNoSchedulesFound: %[ScheduleTable=String][AppID=String] [ClusterID=String][NodeID=String]: No schedules found in DB for directory synchronization.

Explanation No automatic LDAP directory synchronization possible

Recommended Action Check the DirSync configuration

Error Message

%UC_DirSync-6-DirSyncScheduledTaskOver: %[ScheduleID=String][TaskID=String][AppID=String] [ClusterID=String][NodeID=String]: Directory synchronization operation got over.

Explanation Information of the directory synchronization started

Recommended Action No action required

Error Message

%UC_DirSync-4-DirSyncScheduledTaskTimeoutOccured: %[ScheduleID=String][TaskID=String] [AppID=String][ClusterID=String][NodeID=String]: Timeout occurred for directory synchronization task.

Explanation Timeout occurred for directory synchronization task

Recommended Action Check the DirSync configuration

Error Message

%UC_DirSync-3-DirSyncScheduledTaskFailed: %[ScheduleID=String][ErrorMessage=String] [AppID=String][ClusterID=String][NodeID=String]: Directory synchronization task failed.

Explanation Directory synchronization task failed

Recommended Action Check the DirSync configuration and logs

Error Message

%UC_DirSync-3-DirSyncSchedulerFailedToGetDBSchedules: %[Message=String][AppID=String] [ClusterID=String][NodeID=String]: Failed to get directory synchronization schedules from DB.

Explanation Failed to get directory synchronization schedules from DB

Recommended Action Check the DirSync configuration and logs

Error Message

%UC_DirSync-3-DirSyncSchedulerInvalidEventReceived: %[Action=String][Message=String] [AppID=String][ClusterID=String][NodeID=String]: Invalid event received by DirSync scheduler from database.

Explanation Invalid event received by DirSync scheduler from database

Recommended Action Check the DirSync configuration and logs

Error Message

%UC_DirSync-3-DirSyncInvalidScheduleFound: %[ScheduleID=String][AppID=String] [ClusterID=String][NodeID=String]: Invalid schedule read by DirSync scheduler from database.

Explanation Invalid schedule read by DirSync scheduler from database

Recommended Action Check the DirSync configuration and logs

Error Message

%UC_DirSync-3-DirSyncSchedulerFailedToRegisterDBEvents: %[ScheduleTable=String] [AppID=String][ClusterID=String][NodeID=String]: DirSync scheduler failed to register DB notifications.

Explanation Invalid schedule read by DirSync scheduler from database

Recommended Action Check the DirSync configuration and logs

Error Message

%UC_DirSync-3-DirSyncSchedulerEngineFailedToStart: %[ScheduleTable=String][AppID=String]

[ClusterID=String][NodeID=String]: DirSync scheduler engine failed to start.

Explanation DirSync scheduler engine failed to start

Recommended Action Check the DirSync configuration and logs

Error Message

%UC_DirSync-6-DirSyncSchedulerEngineStopped: %[Version=String][AppID=String] [ClusterID=String][NodeID=String]: DirSync scheduler engine stopped.

Explanation DirSync scheduler engine stopped

Recommended Action No action required

Error Message

%UC_DirSync-3-DirSyncScheduleDeletionFailed: %[ScheduleID=String][AppID=String] [ClusterID=String][NodeID=String]: DirSync schedule deletion request failed.

Explanation DirSync schedule deletion request failed

Recommended Action Check the DirSync configuration and logs

Error Message

%UC_DirSync-6-DirSyncNewScheduleInserted: %[ScheduleID=String][AppID=String] [ClusterID=String][NodeID=String]: New schedule inserted in the DirSync Scheduler Engine.

Explanation New schedule inserted in the DirSync Scheduler Engine

Recommended Action No Action Required

Error Message

%UC_DirSync-3-DirSyncScheduleUpdateFailed: %[ScheduleID=String][AppID=String] [ClusterID=String][NodeID=String]: DirSync schedule update request failed.

Explanation DirSync schedule deletion update failed

Recommended Action Check the DirSync configuration and logs

Error Message

%UC_JAVAAPPLICATIONS-6-IPMAStarted: %[ServletName=String][Reason=String][AppID=String] [ClusterID=String][NodeID=String]: IPMA Application started .

Explanation Application started successfully

Recommended Action No action required.

Error Message

%UC_JAVAAPPLICATIONS-3-UserSyncFail: %[Userid=String][Reason=String][AppID=String] [ClusterID=String][NodeID=String]: User is not Synced.

Explanation While updating the data in db for User Db gave exception

Recommended Action Check the reason for exception and proceed accordingly.

Error Message

%UC_JAVAAPPLICATIONS-4-IPMAStopped: %[ServletName=String][Reason=String][AppID=String]

[ClusterID=String][NodeID=String]: IPMA Application stopped.

Explanation Application was unloaded from Tomcat

Recommended Action Check if Tomcat service is up.

Error Message

%UC_JAVAAPPLICATIONS-0-IPMANotStarted: %[ServletName=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: IPMA Application not started.

Explanation Error occurred while starting application

Recommended Action See application logs for error

Error Message

%UC_JAVAAPPLICATIONS-3-IPMAApplicationError: %[ServletName=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: IPMA Application error.

Explanation IPMA application error

Recommended Action See application logs for details

Error Message

%UC_JAVAAPPLICATIONS-4-IPMAManagerLogout: %[ServletName=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: IPMA Manager Logged out.

Explanation IPMA Manager Logged out by application

Recommended Action To re-login the user, click update in the CCMAdmin IPMA Service configuration page for this user.

Error Message

%UC_JAVAAPPLICATIONS-3-IPMAOverloaded: %[ServletName=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: IPMA Application overloaded.

Explanation IPMA application overloaded

Recommended Action See application logs for details

Error Message

%UC_JAVAAPPLICATIONS-3-IPMAFilteringDown: %[ServletName=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: IPMA Application filtering is down.

Explanation IPMA Application filtering is down

Recommended Action Restart Cisco IP Manager Assistant Service

Error Message

%UC_JAVAAPPLICATIONS-6-IPMAInformation: %[ServletName=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: IPMA Information .

Explanation Application information

Recommended Action No action required.

Error Message

%UC_JAVAAPPLICATIONS-6-BDIStarted: %[AppID=String][ClusterID=String][NodeID=String]: BDI Application started .

Explanation Application started successfully

Recommended Action No action required.

Error Message

%UC_JAVAAPPLICATIONS-4-BDIStopped: %[AppID=String][ClusterID=String][NodeID=String]: BDI Application stopped.

Explanation Application was unloaded from Tomcat

Recommended Action Check if Tomcat service is up.

Error Message

%UC_JAVAAPPLICATIONS-0-BDINotStarted: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: BDI Application not started.

Explanation Error occurred while starting application

Recommended Action See application logs for error

Error Message

%UC_JAVAAPPLICATIONS-3-BDIApplicationError: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: BDI Application error.

Explanation BDI application error

Recommended Action See application logs for details

Error Message

%UC_JAVAAPPLICATIONS-3-BDIOverloaded: %[Reason=String][AppID=String][ClusterID=String]

[NodeID=String]: BDI Application overloaded.

Explanation BDI application overloaded

Recommended Action See application logs for details

Error Message

%UC_JAVAAPPLICATIONS-6-WDStarted: %[ServletName=String][Reason=String][AppID=String] [ClusterID=String][NodeID=String]: WebDialer Application started .

Explanation Application started successfully

Recommended Action No action required.

Error Message

%UC_JAVAAPPLICATIONS-4-WDStopped: %[ServletName=String][Reason=String][AppID=String] [ClusterID=String][NodeID=String]: WebDialer Application stopped.

Explanation Application was unloaded from Tomcat

Recommended Action Check if Tomcat service is up.

Error Message

%UC_JAVAAPPLICATIONS-0-WDNotStarted: %[ServletName=String][Reason=String][AppID=String] [ClusterID=String][NodeID=String]: Failed to startup WebDialer application.

Explanation Error occurred while starting application

Recommended Action See application logs for error

Error Message

%UC_JAVAAPPLICATIONS-3-WDApplicationError: %[ServletName=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: WebDialer Application error.

Explanation WebDialer application error

Recommended Action See application logs for details

Error Message

%UC_JAVAAPPLICATIONS-3-WDOverloaded: %[ServletName=String][Reason=String][AppID=String] [ClusterID=String][NodeID=String]: WebDialer Application overloaded.

Explanation WebDialer application overloaded

Recommended Action See application logs for details

Error Message

%UC_JAVAAPPLICATIONS-6-WDInformation: %[ServletName=String][Reason=String][AppID=String] [ClusterID=String][NodeID=String]: WebDialer informational alarm.

Explanation WebDialer application informational alarm

Recommended Action No action required

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoDRFDBAccessFailure: %[Reason=String][AppID=String]

[ClusterID=String][NodeID=String]: DRF process failed to access local database.

Explanation CiscoDirSync failed to access local database

Recommended Action Please make sure the local CallManager database is working properly. The failed sync process will restart at the next scheduled time.

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoDRFMasterAgentStartFailure: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: DRF Master Agent was not able to start.

Explanation DRF Master Agent might be down

Recommended Action Check if the Master Agent is running or port 4040 is in use.

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoDRFLocalAgentStartFailure: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: DRF Local Agent was not able to start.

Explanation DRF Local Agent might be down

Recommended Action Check if the Local Agent is running or port 4343 is in use.

Error Message

%UC_JAVAAPPLICATIONS-6-CiscoDRFLA2MAFailure: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: DRF LA to MA connection has some problems..

Explanation DRF LA to MA connection has some problems.

Recommended Action Check if the Master Agent is up and the port is authorized.

Error Message

%UC_JAVAAPPLICATIONS-6-CiscoDRFMA2LAFailure: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: DRF MA to LA connection has some problems..

Explanation DRF MA to LA connection has some problems.

Recommended Action Check if the Local Agent is up and the port is authorized.

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoDRFBackupFailure: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: DRF Backup process has some problems..

Explanation DRF Backup process has some problems.

Recommended Action Check if the disk is full or tape is not online.

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoDRFRestoreFailure: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: DRF Restore process has some problems..

Explanation DRF Restore process has some problems.

Recommended Action Check if the disk is full or tape is not online.

Error Message

%UC_JAVAAPPLICATIONS-4-CiscoDRFUnknownMessage: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: DRF process has received an unknown message, and discard..

Explanation DRF process has received an unknown message, and discard.

Recommended Action None.

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoDRFDeviceError: %[Reason=String][AppID=String]

[ClusterID=String][NodeID=String]: DRF process has the problem with device..

Explanation DRF process has the problem with device.

Recommended Action Check if the proper device has been defined in the DB.

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoDRFInternalProcessFailure: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: DRF internal process has some problems..

Explanation DRF internal process has some problems.

Recommended Action Check the reason, and restart Master Agent.

Error Message

%UC_JAVAAPPLICATIONS-6-CiscoDRFHistory: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF History Report..

Explanation DRF History Report.

Recommended Action None.

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoDhcpdFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DHCP Daemon stop running..

Explanation DHCP Daemon can't be brought up due to configuration error or crashed when it's running

Recommended Action Check application log for error message and correct the configuration. May require restarting the application if nothing found during the previous steps

Error Message

%UC_JAVAAPPLICATIONS-6-CiscoDhcpdRestarted: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: DHCP Daemon restarted..

Explanation DHCP Daemon restarted successfully.

Recommended Action None.

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoLicenseManagerDown: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: License Manager Down.

Explanation License Manager down - license provisioning will fail

Recommended Action Restart License Manager service on specified node

Error Message

%UC_JAVAAPPLICATIONS-1-CiscoLicenseOverDraft: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: Overdraft licenses in use.

Explanation Overdraft licenses in use

Recommended Action None

Error Message

%UC_JAVAAPPLICATIONS-1-CiscoLicenseApprochingLimit: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: License units consumption approaching its authorized limit.

Explanation License units consumption approaching its authorized limit

Recommended Action None

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoLicenseRequestFailed: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: License Request Unsuccessful.

Explanation License Manager cannot fulfill the license request

Recommended Action See application logs for error

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoLicenseDataStoreError: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: License Database error.

Explanation License application cannot fulfill the request - database error

Recommended Action See application logs for error

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoLicenseInternalError: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: Licensing Internal Error.

Explanation License application internal error

Recommended Action See application logs for error

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoLicenseFileError: %[Reason=String][AppID=String]

[ClusterID=String][NodeID=String]: License File Error.

Explanation Invalid or tampered license file

Recommended Action See application logs, verify that the license file is proper

Error Message

%UC_JAVAAPPLICATIONS-4-CiscoElmNotConnected: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: The system has not synchronized successfully with Enterprise License Manager for many days..

Explanation The system has not synchronized successfully to the Enterprise License Manager.

Recommended Action Check if Enterprise License Manager is connected to the product

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoNoProvisionTimeout: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: The system is operating with an insufficient number of licenses..

Explanation The system is operating with an insufficient number of licenses.

Recommended Action Configure additional licenses in your Enterprise License Manager in order to restore the ability to provision users and devices. Check if Enterprise License Manager is connected to the product.

Error Message

%UC_JAVAAPPLICATIONS-6-CiscoSystemTimeChange: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: System time has changed.

Explanation System Time has changed.

Recommended Action Check why the system time changed

Error Message

%UC_JAVAAPPLICATIONS-6-CiscoGraceTimeLeft: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: Grace period countdown towards no provisioning allowed.

Explanation Grace period countdown towards no provisioning allowed.

Recommended Action Upload additional licenses. Check if Enterprise License Manager is connected to the product.

Error Message

%UC_JAVAAPPLICATIONS-4-CiscoSystemInOverage: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: The system is operating with an insufficient number of licenses..

Explanation The system is operating with an insufficient number of licenses. If additional licenses to cover the shortage are not configured in your Enterprise License Manager within a few days, you will no longer be able to provision users and devices.

Recommended Action Configure additional licenses in your Enterprise License Manager. Check if Enterprise License Manager is connected to the product.

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoSystemSecurityMismatch: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: Due to a certificate mismatch, the system has not synchronized successfully with Enterprise License Manager for many days..

Explanation Certficate Mismatch between Cisco Unified Communications Manager and Enterprise License Manager

Recommended Action Verify Enterprise License Manager certificates. This could be a man-in-the-middle attack.

Error Message

%UC_JAVAAPPLICATIONS-4-CiscoSystemInDemo: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: The system is operating on demo licenses that will expire soon..

Explanation License files have not been uploaded on the Enterprise License Manager.

Recommended Action Upload license files on Enterprise License Manager. Check if Enterprise License Manager is connected to the product.

Error Message

%UC_JAVAAPPLICATIONS-6-CiscoLicenseFileInvalid: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: License File Invalid.

Explanation Invalid license file due to MAC Address

Recommended Action License files need to be rehosted.

Error Message

%UC_JAVAAPPLICATIONS-6-CiscoHardwareLicenseInvalid: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: Invalid / Obsolete Hardware. Cannot upload license files. .

Explanation Installation on invalid / obsolete hardware. Cannot upload license files.

Recommended Action Please obtain correct hardware and re-install.

Error Message

%UC_JAVAAPPLICATIONS-3-DirSyncSchedulerFailedToUpdateNextExecTime: %[Message=String] [AppID=String][ClusterID=String][NodeID=String]: Scheduler failed to update next execution time.

Explanation Scheduler failed to update next execution time

Recommended Action Check the DirSync configuration and logs

Error Message

%UC_JAVAAPPLICATIONS-6-DirSyncScheduleInsertFailed: %[ScheduleID=String][AppID=String] [ClusterID=String][NodeID=String]: DirSync schedule insertion failed.

Explanation DirSync schedule insertion failed

Recommended Action Check the DirSync configuration and logs

Error Message

%UC_JAVAAPPLICATIONS-6-DirSyncSchedulerEngineStarted: %[Version=String][AppID=String] [ClusterID=String][NodeID=String]: DirSync scheduler engine started.

Explanation DirSync scheduler engine started

Recommended Action No action required

Error Message

%UC_JAVAAPPLICATIONS-3-SendEmailAuthenticationError: %[SMTP=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: Unable to autheticate to the SMTP server.

Explanation Unable to autheticate to the SMTP server

Recommended Action See application logs for details

Error Message

%UC_JAVAAPPLICATIONS-3-SendEmailNotificationError: %[SMTP=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: Send Email error.

Explanation Send Email error

Recommended Action See application logs for details

Error Message

%UC_JAVAAPPLICATIONS-3-SendEmailNotificationUnknownError: %[SMTP=String][Reason=String]

[AppID=String][ClusterID=String][NodeID=String]: Send Email error.

Explanation Send Email error

Recommended Action See application logs for details

Error Message

%UC_JAVAAPPLICATIONS-4-DuplicateUserHomeCluster: %[UserID=String][HomeCluster=String] [AppID=String][ClusterID=String][NodeID=String]: User has more than one cluster marked as their home cluster.

Explanation User has more than one cluster marked as their home cluster

Recommended Action Select only one home cluster for a user

Error Message

%UC_JAVAAPPLICATIONS-6-DNAliasServiceStarted: %[AppName=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco Directory Number Alias Service started .

Explanation Application started successfully

Recommended Action No action required.

Error Message

%UC_JAVAAPPLICATIONS-2-DNAliasServiceAllLDAPServersDown: %[AppName=String] [LDAPIpAddress=String][Error=String][AppID=String][ClusterID=String][NodeID=String]: Connectivity to all configured external Call Routing LDAP servers is down.

Explanation Connectivity to all configured external Call Routing LDAP servers is down

Recommended Action No action recommended. The system will try connecting to the server once it is online.

Error Message

%UC_JAVAAPPLICATIONS-3-DNAliasServicePrimaryLDAPServerDown: %[AppName=String] [LDAPIpAddress=String][Error=String][AppID=String][ClusterID=String][NodeID=String]: Connectivity to the configured Primary External Call Routing LDAP server is down .

Explanation Connectivity to the configured Primary External Call Routing LDAP server is down

Recommended Action No action recommended. The system will try connecting to the server once it is online.

Error Message

%UC_JAVAAPPLICATIONS-3-DNAliasServiceSecondaryLDAPServerDown: %[AppName=String] [LDAPIpAddress=String][Error=String][AppID=String][ClusterID=String][NodeID=String]: Connectivity to the configured Secondary External Call Routing LDAP server is down.

Explanation Connectivity to the configured Secondary External Call Routing LDAP server is down

Recommended Action No action recommended. The system will try connecting to the server once it is online.

Error Message

%UC_JAVAAPPLICATIONS-6-DNAliasServicePrimaryLDAPServerOnline: %[AppName=String] [LDAPIpAddress=String][AppID=String][ClusterID=String][NodeID=String]: The configured Primary External Call Routing LDAP server is online and connected.

Explanation The configured Primary External Call Routing LDAP server is online and connected

Recommended Action No recommended action

Error Message

%UC_JAVAAPPLICATIONS-6-DNAliasServiceSecondaryLDAPServerOnline: %[AppName=String] [LDAPIpAddress=String][AppID=String][ClusterID=String][NodeID=String]: The configured Secondary External Call Routing LDAP server is online and connected.

Explanation The configured Secondary External Call Routing LDAP server is online and connected

Recommended Action No recommended action

Error Message

%UC_JAVAAPPLICATIONS-6-DNAliasServiceLDAPSearchFailed: %[AppName=String] [LDAPIpAddress=String][UID=String][Error=String][AppID=String][ClusterID=String] [NodeID=String]: Search operation from the External Call Routing LDAP server failed.

Explanation The Directory Number queried is not found in the External Call Routing LDAP server

Recommended Action No recommended actions if connectivity to all the configured External Call Routing LDAP servers are intact

Error Message

%UC_JAVAAPPLICATIONS-4-DNAliasServiceImproperLDAPFormat: %[AppName=String] [LDAPIpAddress=String][ErrorType=String][AppID=String][ClusterID=String] [NodeID=String]: Malformed LDAP response from the External Call Routing LDAP server.

Explanation Malformed LDAP response from the External Call Routing LDAP server

Recommended Action Network admin should examine the External Call Routing LDAP database and take necessary corrective action

Error Message

%UC_JAVAAPPLICATIONS-2-DNAliasServiceUnauthorizedAccessToLDAPServer: % [AppName=String][LDAPIpAddress=String][ErrorType=String][AppID=String][ClusterID=String] [NodeID=String]: Unauthorized access attempt to the External Call Routing LDAP server.

Explanation Three consecutive unsuccessful bind attempts within 30 seconds to the External Call Routing LDAP server

Recommended Action Network admin should examine the External Call Routing LDAP database and take necessary corrective action

Error Message

%UC_JAVAAPPLICATIONS-4-DNAliasServiceErrorThresholdExceeded: %[AppName=String] [LDAPIpAddress=String][ErrorType=String][AppID=String][ClusterID=String][NodeID=String]: Too many errors from the configured External Call Routing LDAP server.

Explanation The number of errors of all kinds from the External Call Routing LDAP server have exceeded the threshold

Recommended Action Network admin should examine the External Call Routing LDAP database and take necessary corrective action

Error Message

%UC_JAVAAPPLICATIONS-4-DNAliasServiceLDAPAddFailed: %[AppName=String] [LDAPIpAddress=String][UID=String][Error=String][AppID=String][ClusterID=String] [NodeID=String]: Add operation to the External Call Routing LDAP server failed.

Explanation The Directory Number Alias record could not be added to the External Call Routing LDAP server

Recommended Action Network admin should examine the External Call Routing LDAP database and take necessary corrective action

Error Message

%UC_JAVAAPPLICATIONS-4-DNAliasServiceLDAPUpdateFailed: %[AppName=String] [LDAPIpAddress=String][UID=String][Error=String][AppID=String][ClusterID=String] [NodeID=String]: Update operation to the configured External Call Routing LDAP server failed.

Explanation The Directory Number Alias record in the External Call Routing LDAP server could not be updated

Recommended Action Network admin should examine the External Call Routing LDAP database and take necessary corrective action

Error Message

%UC_JAVAAPPLICATIONS-4-DNAliasServiceLDAPDeleteFailed: %[AppName=String] [LDAPIpAddress=String][UID=String][Error=String][AppID=String][ClusterID=String] [NodeID=String]: Delete operation to the configured External Call Routing LDAP server failed.

Explanation The Directory Number Alias record in the External Call Routing LDAP server could not be deleted

Recommended Action Network admin should examine the External Call Routing LDAP database and take necessary corrective action

Error Message

%UC_JAVAAPPLICATIONS-4-DNAliasServiceLDAPTimeExceeded: %[AppName=String] [LDAPIpAddress=String][Operation=String][Time=String][AppID=String][ClusterID=String] [NodeID=String]: Time limit to perform an LDAP operation exceeded.

Explanation The LDAP operation has exceeded the time limit set for its successful completion

Recommended Action Network admin should examine the External Call Routing LDAP database and take necessary corrective action

Error Message

%UC_JAVAAPPLICATIONS-2-DNAliasServiceInitiatingFailover: %[AppName=String] [LDAPIpAddress=String][ToLDAPIpAddress=String][AppID=String][ClusterID=String] [NodeID=String]: Failover initiated from the current External Call Routing LDAP server to the next External Call Routing LDAP server.

Explanation Failover initiated from the current External Call Routing LDAP server to the next External Call Routing LDAP server

Recommended Action Network admin should examine the External Call Routing LDAP database and take necessary corrective action

Error Message

%UC_JAVAAPPLICATIONS-5-DNAliasServiceInitiatingFailback: %[AppName=String] [LDAPIpAddress=String][ToLDAPIpAddress=String][AppID=String][ClusterID=String] [NodeID=String]: Failback initiated from the current External Call Routing LDAP server to the previous External Call Routing LDAP server.

Explanation Failback initiated from the current External Call Routing LDAP server to the previous External Call Routing LDAP server

Recommended Action No recommended action

Error Message

%UC_JAVAAPPLICATIONS-6-DNAliasServiceStopped: %[AppName=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco Directory Number Alias Service stopped .

Explanation Application stopped successfully

Recommended Action No action required.

Error Message

%UC_JAVAAPPLICATIONS-2-DNAliasServiceWatchdogInitRestart: %[AppName=String] [AppID=String][ClusterID=String][NodeID=String]: Cisco Directory Number Alias Service Restarting.

Explanation Application is being restarted due to too many unresponsive threads.

Recommended Action Please note the time stamp when the alarm is raised, collect the logs corresponding to the time stamp using either CLI or RTMT and contact Cisco TAC for support. CLI : "file search activelog cm/trace/dnaliassync/log4j time stamp" gives the file number and "file get activelog /cm/trace/dnaliassync/log4j/log-name" is to be run to get the files. RTMT : follow the path "Trace Log Central > Remote Browse > Cisco Directory Number Alias Sync" and select the files corresponding to the time stamp.

Error Message

%UC_JAVAAPPLICATIONS-3-DNAliasServiceNewProcessingThreadStarted: %[AppName=String] [Cause=String][AppID=String][ClusterID=String][NodeID=String]: Cisco Directory Number Alias Service has initiated a new thread.

Explanation Application has started a new instance of the main Processing Thread as the previous instance was detected to be hung and out of service.

Recommended Action Network admin should contact Cisco TAC for support if the problem persists and this alarm is issued more than 5 times after the service is started.

Error Message

%UC_JAVAAPPLICATIONS-3-SmartCallHomeMessageSendFailed: %[MessageName=String][MessageDetail=String][AppID=String][ClusterID=String][NodeID=String]: This alarm will be raised when call home messages do not reach Cisco backend server due to one of the below condtions mentioned : 1) User selected Secure Web(HTTPS) option in 'Send to TAC' field for sending the messages : Smart Call Home backend server is down/unreachable or DNS settings done by the user are not correct.2) User selected email option in 'Send to TAC' field for sending the messages : SMTP server is down/unreachable or is not configured correctly so the messages did not reach Smart Call Home backend server.3) User selected Secure Web(HTTPS) through Proxy option in 'Send to TAC' field for sending the messages : Proxy settings are not correct or Proxy server is unreachable so the messages did not reach Smart Call Home backend server..

Explanation Smart Call Home messages could not be sent to SCH backend server due to connectivity issues

Recommended Action 1) Please check if DNS is configured and reachable and you have valid certificates if you are using Secure Web(HTTPS) option for sending Smart Call Home Messages.2) Please check if SMTP server is configured and reachable if you are using email option for sending Smart Call Home Messages.3) Please check if Proxy server is up and running if you are using Secure Web(HTTPS) through Proxy option for sending Smart Call Home Messages

Error Message

%UC_JAVAAPPLICATIONS-6-CiscoDirSyncProcessCompletedWithError: %[AgreementId=String][Reason=String][AppID=String][ClusterID=String][NodeID=String]: LDAPSync process completed on particular sync agreement with errors

Explanation Completed LDAP sync with some errors. Please check the logs for more details.

Recommended Action No action required

Error Message

%UC_JAVAAPPLICATIONS-3-JabberClientAlarm: %[Type=String][ErrorDescription=String][TrackingId=String][SessionId=String][UserJid=String][OtherInfo=String][AppID=String][ClusterID=String][NodeID=String]: This is an alarm generated by Jabber Client

Explanation There was an error that occurred on Jabber Client side

Recommended Action Refer to the Type, Error Description fields for more details

Error Message

%UC_JAVAAPPLICATIONS-6-CiscoDirSyncZeroOrgsSynced: %[AgreementId=String][Reason=String][AppID=String][ClusterID=String][NodeID=String]: This is alarm to indicate the ldapsearch resulted in zero orgs when searched

Explanation Unable to fetch any orgs from LDAP server. Please check the logs for more details.

Recommended Action Please check DirSync logs for more information on LDAP search results and also how the entries are configured on the LDAP server

Error Message

%UC_JAVAAPPLICATIONS-3-CiscoDirSyncOrgFetchFailedForUser: %[AgreementId=String][UserId=String][AppID=String][ClusterID=String][NodeID=String]: This is alarm to indicate the ldapsearch resulted in zero orgs for user

Explanation Unable to fetch any orgs from LDAP server. Please check the logs for more details.

Recommended Action Please check DirSync logs for more information on LDAP search results and also how the entries are configured on the LDAP server

Error Message

%UC_JAVAAPPLICATIONS-6-DevActStarted: %[ServletName=String][Reason=String][AppID=String][ClusterID=String][NodeID=String]: Device Activation Application started

Explanation Unable to fetch any orgs from LDAP server. Please check the logs for more details.

Recommended Action Please check DirSync logs for more information on LDAP search results and also how the entries are configured on the LDAP server

Error Message

%UC_JAVAAPPLICATIONS-4-DevActStopped: %[ServletName=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: Device Activation Application stopped

Explanation Application was unloaded from Tomcat

Recommended Action Check if Tomcat service is up.

Error Message

%UC_JAVAAPPLICATIONS-3-DevActApplicationError: %[ServletName=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: Device Activation Application error

Explanation Device activation application error

Recommended Action See application logs for details

Error Message

%UC_JAVAAPPLICATIONS-3-DevActApplicationOnboardFailure: %[ServletName=String] [Reason=String][IP=String][AppID=String][ClusterID=String][NodeID=String]: Device Activation Failed

Explanation An attempt to activate an IP Phone using an activation code has failed. Refer to the "Reason" parameter for a specific cause of the failure. This failure has invalidated the activation code that was used.

Recommended Action Generate a new activation code before retrying the device on-boarding.

Error Message

%UC_JAVAAPPLICATIONS-6-DevActInformation: %[ServletName=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: Device activation informational alarm

Explanation Device activation application informational alarm

Recommended Action No action required

Error Message

%UC_CEF-4-QRTRequest: %[Category=String][ReasonCode=String][TimeStamp=String] [DeviceName=String][IPAddress=String][DN=String][AppID=String][ClusterID=String] [NodeID=String]: User submitted problem report using Quality Report Tool..

Explanation Application started successfully

Recommended Action No action required.

Error Message

%UC_RTMT-3-RTMT_ALERT: %[AlertName=String][AlertDetail=String][AppID=String] [ClusterID=String][NodeID=String]: RTMT Alert.

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

Recommended Action Check AlertCentral in RTMT or any alerts that you have received via 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.

Error Message

%UC_RTMT-3-AlertEmailNotifyFailure: %[FailureReason=String][AppID=String][ClusterID=String][NodeID=String]: Alert Email Notification Failure..

Explanation Alert notification mechanism using e-mails has failed.

Recommended Action Email notification of alerts failed due to a mis-configured SMTP Settings/SMTP server down. Check SMTP Server configuration and Examine the AMC service log files to determine the exact reason for failure.

Error Message

%UC_RTMT-3-ServiceabilityConnectivityInterruptions: %[AdditionalInformation=String][AppID=String][ClusterID=String][NodeID=String]: Serviceability connectivity interruptions have been detected in the cluster.

Explanation Connectivity interruptions have been detected in the cluster. These connectivity interruptions can result in generation of incorrect notifications and alerts.

Recommended Action Connectivity interruptions have occurred because of underlying network issues. Communication streams between the ports involved needs to be analyzed to determine the exact cause of failure. The CLI command "utils network capture" or third-party tools can be used to capture the packet stream between the ports for analysis.

Error Message

%UC_CDRREP-3-CDRFileDeliveryFailed: %[BillingServerAddress=String][AppID=String][ClusterID=String][NodeID=String]: (s)FTP delivery of CDR files to the outside billing server failed..

Explanation (s)FTP develiry of CDR files to the Billing Server outside of the cluster failed because of timeout or other reasons. Email alert will be sent to the admin.

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.

Error Message

%UC_CDRREP-3-CDRAgentSendFileFailed: %[CDRRepositoryNodeAddress=String][CDRAgentNodeAddress=String][AppID=String][ClusterID=String][NodeID=String]: CDR Agent cannot send CDR files from CCM node to CDR Repository node within the CCM cluster.

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

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.

Error Message

%UC_CDRREP-4-CDRHWMExceeded: %[DiskUsageInMB=String][AppID=String][ClusterID=String][NodeID=String]: High Water Mark for CDR files reached, some successfully delivered CDR files have been deleted.

Explanation 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. Email alert will be sent to the admin.

Recommended Action 1. The preservation duration may be too long. Reduce it at Serviceability->Tools->CDR Management. 2. Or to raise maximum allocated disk space and/or HWM for CDR files.

Error Message

%UC_CDRREP-2-CDRMaximumDiskSpaceExceeded: %[DiskUsageInMB=String][AppID=String][ClusterID=String][NodeID=String]: The CDR files disk usage exceeded maximum disk allocation. Some undelivered files may have been deleted to bring disk usage down..

Explanation 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 undelivered files or not depends on how deletionDisable flag is configured at CDRM Configuration page. Email alert will be sent to the admin.

Recommended Action 1. Check if there are too many undelivered 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.

Error Message

%UC_CDRREP-3-CDRFileDeliveryFailureContinues: %[BillingServerAddress=String][AppID=String][ClusterID=String][NodeID=String]: (s)FTP delivery of CDR files failed on retries..

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

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.

Error Message

%UC_CDRREP-3-CDRAgentSendFileFailureContinues: %[CDRRepositoryNodeAddress=String][CDRAgentNodeAddress=String][AppID=String][ClusterID=String][NodeID=String]: CDR Agent cannot send CDR files from CCM node to CDR Repository node on retries..

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

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.

Error Message

%UC_null-6-TestAlarmInformational: %[AppID=String][ClusterID=String][NodeID=String]: Testing INFORMATIONAL_ALARM .

Explanation Test Alarm

Recommended Action No action required.

Error Message

%UC_null-0-TestAlarmEmergency: %[AppID=String][ClusterID=String][NodeID=String]: Testing EMERGENCY_ALARM .

Explanation Test Alarm

Recommended Action No action required.

Error Message

%UC_null-1-TestAlarmAlert: %[AppID=String][ClusterID=String][NodeID=String]: Testing ALERT_ALARM .

Explanation Test Alarm

Recommended Action No action required.

Error Message

%UC_null-2-TestAlarmCritical: %[AppID=String][ClusterID=String][NodeID=String]: Testing CRITICAL_ALARM .

Explanation Test Alarm

Recommended Action No action required.

Error Message

%UC_null-7-TestAlarmDebug: %[AppID=String][ClusterID=String][NodeID=String]: Testing DEBUG_ALARM .

Explanation Test Alarm

Recommended Action No action required.

Error Message

%UC_null-3-TestAlarmError: %[AppID=String][ClusterID=String][NodeID=String]: Testing ERROR_ALARM .

Explanation Test Alarm

Recommended Action No action required.

Error Message

%UC_null-5-TestAlarmNotice: %[AppID=String][ClusterID=String][NodeID=String]: Testing NOTICE_ALARM .

Explanation Test Alarm

Recommended Action No action required.

Error Message

%UC_null-4-TestAlarmWarning: %[AppID=String][ClusterID=String][NodeID=String]: Testing

WARNING_ALARM .

Explanation Test Alarm

Recommended Action No action required.

Error Message

%UC_null-6-TestAlarmAppliance: %[AppID=String][ClusterID=String][NodeID=String]: Testing INFORMATIONAL_ALARM .

Explanation Test Alarm for Appliance OS based server Only.

Recommended Action No action required.

Error Message

%UC_SYSACC-4-TotalProcessesAndThreadsExceededThresholdStart: %[NumberOfProcesses=String] [NumberOfThreads=String][Reason=String][ProcessWithMostInstances=String] [ProcessWithMostThreads=String][AppID=String][ClusterID=String][NodeID=String]: 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..

Explanation The current total number of processes and threads has exceeded the maximum number of tasks. This situation could indicate some process is leaking or some process has thread leaking.

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 (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 recommended actions 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 RIS Data Collector, Cisco AMC Service, and Cisco RIS Perfmon Logs and contact Cisco Technical Assistance Center (TAC) for detailed assistance.

Error Message

%UC_SYSACC-5-TotalProcessesAndThreadsExceededThresholdEnd: %[NumberOfProcesses=String] [NumberOfThreads=String][Reason=String][AppID=String][ClusterID=String][NodeID=String]: 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..

Explanation The current total number of processes and threads is less than the maximum number of tasks that has been 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.

Recommended Action This alarm is for information purposes only; no action is required.

Error Message

%UC_DRF-3-DRFTruststoreMissing: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF uses ipsec truststore certificate for securing communication between the MA and LA service. This certificate is missing on the node.

Explanation 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

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.

Error Message

%UC_DRF-3-DRFUnknownClient: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: 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.

Explanation 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.

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

Error Message

%UC_DRF-3-DRFSecurityViolation: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: The DRF System has detected a malicious pattern which could result in a security violation.

Explanation 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.

Recommended Action Stop the Cisco DRF Master and Cisco DRF Local Agent Services

Error Message

%UC_DRF-3-DRFMasterAgentStartFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF Master Agent was unable to start because it was unable to open port 4040..

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

Recommended Action Check if port 4040 is not already in use.

Error Message

%UC_DRF-3-DRFLocalAgentStartFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF Local Agent was not able to start because it was unable to connect to the Master Agent on port 4040.

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

Recommended Action Check if the CiscoDRFMaster and CiscoDRFLocal services are running

Error Message

%UC_DRF-3-DRFLA2MAFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF Local Agent is not able to connect to Master Agent..

Explanation DRF Local Agent is not able to connect to Master Agent.

Recommended Action Check if the Master Agent is up and the port is authorized.

Error Message

%UC_DRF-3-DRFMA2LAFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: Master Agent was unable to send a backup/restore request to the local agent..

Explanation Master Agent was unable to send a backup/restore request to the local agent.

Recommended Action Restart the corresponding local agents and the master agent.

Error Message

%UC_DRF-3-DRFBackupFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: Cisco DRF Backup process failed..

Explanation DRF Backup process encountered errors.

Recommended Action Check DRF logs for further details.

Error Message

%UC_DRF-3-DRFRestoreFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF Restore process failed..

Explanation DRF Restore process encountered errors.

Recommended Action Check DRF logs for further details.

Error Message

%UC_DRF-3-DRFBackupDeviceError: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF Backup process is failed due to backup device error..

Explanation DRF Backup process is failed due to backup device error.

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

Error Message

%UC_DRF-3-DRFTapeDeviceError: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF is unable to access tape device..

Explanation DRF is unable to access tape device.

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

Error Message

%UC_DRF-3-DRFLocalDeviceError: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF is unable to access local device..

Explanation DRF is unable to access local device.

Recommended Action Check if local location exists and is accessible.

Error Message

%UC_DRF-3-DRFInternalProcessFailure: %[Reason=String][AppID=String][ClusterID=String]

[NodeID=String]: DRF internal process has encountered an error..

Explanation DRF internal process has encountered an error.

Recommended Action Check DRF logs for details.

Error Message

%UC_DRF-3-DRFRestoreInternalError: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF Restore operation has encountered an error. Restore cancelled internally..

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

Recommended Action Check DRF logs for details.

Error Message

%UC_DRF-3-DRFMABackupComponentFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF was unable to backup at least one component..

Explanation DRF requested a component to backup its' data. However, there was an error during the backup process and the component was not backed up.

Recommended Action Please check the component backup logs and contact support if needed.

Error Message

%UC_DRF-3-DRFMARestoreComponentFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF was unable to restore at least one component..

Explanation DRF requested a component to restore its' data. However, there was an error during the restore process and the component was not restored.

Recommended Action Please check the component restore logs and contact support if needed.

Error Message

%UC_DRF-3-DRFMABackupNodeDisconnect: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: The node being backed up disconnected from the Master Agent prior to being fully backed up..

Explanation 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.

Recommended Action Please check the computer that disconnected during backup. If the computer was accidentally shutdown, restart the backup.

Error Message

%UC_DRF-3-DRFNoRegisteredComponent: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: No registered components available, backup failed..

Explanation DRF backup failed since no registered components are available.

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

Error Message

%UC_DRF-3-DRFNoRegisteredFeature: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: No feature selected for backup..

Explanation No feature selected for backup

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

Error Message

%UC_DRF-3-DRFMARestoreNodeDisconnect: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: The node being restored disconnected from the Master Agent prior to being fully restored..

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

Recommended Action Please check the computer that disconnected during restore. If the computer was accidentally shutdown, restart the restore.

Error Message

%UC_DRF-3-DRFSftpFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF sftp operation has failed..

Explanation DRF sftp operation has failed.

Recommended Action Ensure that the destination server is available, has appropriate permissions and sftp daemon is running.

Error Message

%UC_DRF-3-DRFRegistrationFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF Registration operation failed..

Explanation DRF Registration operation failed.

Recommended Action DRF Registration failed for a component due to some internal error. Check the DRF logs and contact support if needed.

Error Message

%UC_DRF-3-DRFBackupCancelInternalError: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF Backup operation has encountered an error. Backup cancelled internally..

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

Recommended Action Check DRF logs for details.

Error Message

%UC_DRF-4-DRFLogDirAccessFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF couldn't access the log directory..

Explanation DRF couldn't access the log directory.

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

Error Message

%UC_DRF-4-DRFComponentDeRegistered: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF succesfully de-registered the requested component..

Explanation DRF succesfully de-registered the requested component.

Recommended Action Ensure that the component deregistered is not needed for further backup/restore operation.

Error Message

%UC_DRF-4-DRFDeRegistrationFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF de-registration request for a component failed..

Explanation DRF de-registration request for a component failed.

Recommended Action Please check the DRF logs and contact support if needed.

Error Message

%UC_DRF-4-DRFDeRegisteredServer: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF automatically de-registered all the components for a server..

Explanation This server might have got disconnected from CCM cluster.

Recommended Action Nothing.

Error Message

%UC_DRF-4-DRFSchedulerDisabled: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF Scheduler is disabled because no configured features available for backup..

Explanation DRF Scheduler is disabled because no configured features available for backup.

Recommended Action Ensure at least one feature is configured for the scheduled backup to run.

Error Message

%UC_DRF-6-DRFComponentRegistered: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF Succesfully Registered the requested component..

Explanation DRF Succesfully Registered the requested component.

Recommended Action Ensure that the registered component is needed for backup/restore operation.

Error Message

%UC_DRF-6-DRFSchedulerUpdated: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF Scheduled backup configurations is updated automatically due to feature DeRegistration..

Explanation DRF Scheduled backup configurations is updated automatically due to feature DeRegistration.

Recommended Action Ensure that the new configurations is appropriate one for the backup/restore operation.

Error Message

%UC_DRF-6-DRFBackupCompleted: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF backup completed successfully..

Explanation DRF backup completed successfully.

Recommended Action Ensure that the backup operation completed successfully.

Error Message

%UC_DRF-6-DRFRestoreCompleted: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: DRF restore completed successfully..

Explanation DRF restore completed successfully.

Recommended Action Ensure that the restore operation completed successfully.

Error Message

%UC_DRF-3-DRFFailure: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: DRF Backup or Restore process has failed..

Explanation DRF Backup or Restore process encountered errors.

Recommended Action Check DRF logs for further details.

Error Message

%UC_DRF-4-DRFNoBackupTaken: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: A valid backup of the current system was not found..

Explanation A valid backup of the current system was not found after an Upgarde/Migration or Fresh Install.

Recommended Action It is recommended to perform a Backup using the Disaster Recovery System.

Error Message

%UC_LOGIN-4-AuthenticationFailed: %[LoginFrom=String][TimeStamp=String][UserID=String] [Interface=String][AppID=String][ClusterID=String][NodeID=String]: Login Authentication failed..

Explanation Authentication failure for login attempt is detected.

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

Error Message

%UC_LOGIN-6-AuthenticationSucceeded: %[LoginFrom=String][TimeStamp=String][UserID=String] [Interface=String][AppID=String][ClusterID=String][NodeID=String]: Login Authentication succeeded..

Explanation Authentication success for login attempt is detected.

Recommended Action If this event is expected, no action is required; otherwise, notify the administrator.

Error Message

%UC_CERT-6-CertExpiryApproaching: %[Message=String][AppID=String][ClusterID=String] [NodeID=String]: Information Alarm that Indicates a Certificate Validity Period is approaching and the expiry date is within the notification window configured .

Explanation Certificate Expiry Date is approaching shortly and Certificate is going to be invalid.

Recommended Action Re-generate the certificate that is about to Expire from Certificate Management UI from CUOS Administration web Page. If the Certificate is issued by a CA, Generate a CSR, Submit CSR to CSA ,obtain a fresh certificate from CA and upload it to CUCM

Error Message

%UC_CERT-0-CertExpired: %[Message=String][AppID=String][ClusterID=String] [NodeID=String]: Certificate has Expired and needs to be changed at the earliest.

Explanation The Validity Date of the Certificate indicated is over and the Certificate is expired.

Recommended Action Re-generate the certificate that is about to Expire from Certificate Management UI from CUOS Administration web Page. If the Certificate is issued by a CA, obtain a fresh certificate from CA and upload it to CUCM.

Error Message

%UC_CERT-1-CertValidLessthanADay: %[Message=String][AppID=String][ClusterID=String] [NodeID=String]: Certificate is about to Expire in less than 24 hours or has Expired .

Explanation The Validity of the Certificate indicated in the notification message is less than 24 hours .

Recommended Action Re-generate the certificate that is about to Expire from Certificate Management UI from CUOS Administration web Page. If the Certificate is issued by a CA, Generate a CSR, Submit CSR to CA, obtain a fresh certificate from CA and upload it to CUCM

Error Message

%UC_CERT-2-CertValidfor7days: %[Message=String][AppID=String][ClusterID=String] [NodeID=String]: Alarm to indicate that Certificate has Expired or Expires in less than seven days.

Explanation The Certifciate is invalid or Validity of the Certificate indicated in the notification less than 7 days.

Recommended Action Re-generate the certificate that is about to Expire from Certificate Management UI from CUOS Administration web Page. If the Certificate is issued by a CA, Generate a CSR, Submit CSR to CA, obtain a fresh certificate from CA and upload it to CUCM

Error Message

%UC_CERT-5-CertValidityOver30Days: %[Message=String][AppID=String][ClusterID=String] [NodeID=String]: Alarm to Indicate certificate to Expiry is approaching but expiry date is more than 30 days .

Explanation Information Alarm that Indicates a Certificate Validity Period is approaching and validity of certificate is more than 30 days

Recommended Action Re-generate the certificate that is about to Expire from Certificate Management UI from CUOS Administration web Page. If the Certificate is issued by a CA, Generate a CSR, Submit CSR to CA, obtain a fresh fresh certificate from CA and upload it to CUCM

Error Message

%UC_CERT-4-CertValidLessThanMonth: %[Message=String][AppID=String][ClusterID=String][NodeID=String]: Alarm that indicates Certificate Expire in 30 days or lesser .

Explanation The Expiry date of the Certificate indicated in the notification is less than a month

Recommended Action Re-generate the certificate that is about to Expire from Certificate Management UI from CUOS Administration web Page. If the Certificate is issued by a CA, Generate a CSR, Submit CSR to CA, obtain a fresh certificate from CA and upload it to CUCM.

Error Message

%UC_CERT-2-TomcatCertRegen: %[Message=String][AppID=String][ClusterID=String][NodeID=String]: Alarm that indicates the tomcat certificate is regenerated.

Explanation This alarm indicates that tomcat certificate has been regenerated or CA signed Tomcat Certificate has been uploaded.

Recommended Action Restart the tomcat service for the new tomcat certificate to be effective. If EMCC feature is enabled for the communication across the clusters, perform the bulk certificate management provisioning for tomcat unit from Cisco Unified OS Administration Webpage

Error Message

%UC_CERT-0-CertificateRevoked: %[Message=String][AppID=String][ClusterID=String][NodeID=String]: Alarm indicates that recently uploaded certificate is revoked and needs to be changed at the earliest..

Explanation This alarm indicates that recently uploaded third party signed certificate or trust certificate is revoked.

Recommended Action Delete revoked trust certificate and re-upload it from Cisco Unified OS Administration Webpage. In case of third party signed (own) certifiate, just re-upload new certificate.

Error Message

%UC_CERT-4-CertificateRevokationStatusByOCSP: %[Message=String][AppID=String][ClusterID=String][NodeID=String]: Alarm indicates that CUCM could not determine OCSP revocation status of recently uploaded certificate..

Explanation This alarm indicates that CUCM failed to determine revocation status of recently uploaded third party signed certificate or trust certificate.

Recommended Action Evaluate reason of certificate revocation failure. Delete and re-upload certificate if required.

Error Message

%UC_CERT-4-ITLRecoveryCertBackup: %[Message=String][AppID=String][ClusterID=String][NodeID=String]: This cluster has an ITLRecovery certificate that has not been backed up. Taking a manual backup of this certificate is recommended to avoid the need to manually delete the ITL file from every phone in the cluster after certain cluster reconfiguration operations..

Explanation This alarm indicates that the newly generated ITL Recovery Certificate and key have not yet been backed up.

Recommended Action Use the CLI command "file get tftp ITLRecovery.p12" to back up the ITL Recovery Certificate as soon as possible.

Error Message

%UC_CERT-3-CertExpired: %[Message=String][AppID=String][ClusterID=String][NodeID=String]: This indicates certificate has expired. Please renew the certificate at the earliest.

Explanation This alarm indicates that certificate has expired

Recommended Action Renew the certificate at the earliest.

Error Message

%UC_IMS-4-authFail: %[UserID=String][Message=String][AppID=String][ClusterID=String] [NodeID=String]: An attempt to authenticate this user with the given credentials failed..

Explanation Failed to authenticate this user.

Recommended Action Determine correct credentials and retry.

Error Message

%UC_IMS-4-SSONullTicket: %[Message=String][AppID=String][ClusterID=String][NodeID=String]: A null ticket was passed..

Explanation Failed to authenticate this user.

Recommended Action Get non null ticket and retry.

Error Message

%UC_IMS-4-SSOServerUnreachable: %[Message=String][AppID=String][ClusterID=String] [NodeID=String]: SSO server could not be reached..

Explanation SSO server could not be reached.

Recommended Action Check reachability to SSO server.

Error Message

%UC_IMS-3-LDAPServerUnreachable: %[LDAPUrl=String][AppID=String][ClusterID=String] [NodeID=String]: Authentication server could not be reached..

Explanation Authentication server could not be reached.

Recommended Action Check reachability to Authentication server.

Error Message

%UC_IMS-4-SSOuserNotInDB: %[Message=String][AppID=String][ClusterID=String] [NodeID=String]: User was not found in DB..

Explanation User was not found in DB.

Recommended Action Perform sync manually or wait till next scheduled sync.

Error Message

%UC_IMS-4-SSODisabled: %[Message=String][AppID=String][ClusterID=String] [NodeID=String]: SSO disabled on CUCM..

Explanation SSO disabled on CUCM.

Recommended Action run CLI command to enable SSO.

Error Message

%UC_IMS-4-SSOInternal: %[Message=String][AppID=String][ClusterID=String]

[NodeID=String]: Failedto open a file..

Explanation Failed to authenticate this user.

Recommended Action Try again after some time.

Error Message

%UC_IMS-6-authSuccess: %[UserID=String][AppID=String][ClusterID=String][NodeID=String]: User successfully authenticated..

Explanation Successfully authenticated this user.

Recommended Action No action required.

Error Message

%UC_IMS-4-authLdapInactive: %[UserID=String][AppID=String][ClusterID=String] [NodeID=String]: Authentication failed due to the user existing in the local database, but system is configured for LDAP authentication..

Explanation A directory sync was likely done in the immediate past (1 day), This user has yet to be removed from the database. No action should be necessary. This should clear itself within 24 hours.

Recommended Action No action should be necessary.

Error Message

%UC_IMS-4-authAdminLock: %[UserID=String][AppID=String][ClusterID=String][NodeID=String]: The Administrator has locked this credential, therfore the authentication failed..

Explanation User is locked out by administrator.

Recommended Action Administrator may unlock this credential.

Error Message

%UC_IMS-4-authHackLock: %[UserID=String][AppID=String][ClusterID=String][NodeID=String]: This user attempted to login unsuccessfully the number of times set by the administrator. At that time the credential is locked..

Explanation User attempted too many incorrect authentications in the time frame set by the administrator.

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

Error Message

%UC_IMS-5-authExpired: %[UserID=String][AppID=String][ClusterID=String][NodeID=String]: The authentication failed because this credential has expired..

Explanation This user's credentials have expired.

Recommended Action Administrator may reset the credential.

Error Message

%UC_IMS-4-authInactiveLock: %[UserID=String][AppID=String][ClusterID=String] [NodeID=String]: Authentication failed because the credential is locked due to inactivity..

Explanation User has been inactive for the administrator specified time. The credential is locked.

Recommended Action Administrator may reset the credential.

Error Message

%UC_IMS-5-authMustChange: %[UserID=String][AppID=String][ClusterID=String] [NodeID=String]: Authentication failed because it is marked that it must be changed by the user at this time..

Explanation User Must Change is set on this credential. The user can gain access after changing the credential.

Recommended Action User or Administrator may reset credential.

Error Message

%UC_IMS-6-credUpdateFailure: %[UserID=String][AppID=String][ClusterID=String] [NodeID=String]: There are a number of reasons an update of a credential could fail. Likely cause is that the credential doesn't pass security requirements (too short for example), has been used previously, etc..

Explanation Some problem updating the credential.

Recommended Action Determine issue (check length requirements, etc.) for this credential and retry.

Error Message

%UC_IMS-6-credUpdateSuccess: %[UserID=String][AppID=String][ClusterID=String] [NodeID=String]: The credential has been updated..

Explanation Credential was successfully updated.

Recommended Action No action required.

Error Message

%UC_IMS-6-credFullUpdateSuccess: %[Message=String][AppID=String][ClusterID=String] [NodeID=String]: Fields associated with this credential have been successfully updated..

Explanation Credential was successfully updated.

Recommended Action No action required.

Error Message

%UC_IMS-6-credFullUpdateFailure: %[Message=String][AppID=String][ClusterID=String] [NodeID=String]: The update for the fields associated with this credential failed..

Explanation An error was encountered during update of credential fields.

Recommended Action Determine issue and retry.

Error Message

%UC_IMS-5-credReadFailure: %[UserID=String][Message=String][AppID=String][ClusterID=String] [NodeID=String]: Some error was encountered when attempting to read credential from the database. This could be a network or database issue..

Explanation Error occured attempting to read a credential.

Recommended Action Ensure credential (user name) exists. Could be database problem.

Error Message

%UC_IMS-6-credReadSuccess: %[UserID=String][AppID=String][ClusterID=String] [NodeID=String]: This credential was successfully accessed from the databse..

Explanation Successfully read a credential.

Recommended Action No action required.

Error Message

%UC_IMS-6-AdminPassword: %[Message=String][AppID=String][ClusterID=String] [NodeID=String]: Administrative password changed successfully, or unsuccessfully based on message displayed..

Explanation Password change succeeded or failed based on message displayed.

Recommended Action No further recommendation.

Error Message

%UC_CAR-3-CARSchedulerJobFailed: %[JobName=String][FailureCause=String][FailureDetail=String] [AppID=String][ClusterID=String][NodeID=String]: Critical CAR scheduled job failed..

Explanation A critical CAR scheduled job failed for some reasons.

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.

Error Message

%UC_CAR-3-CARSchedulerJobError: %[JobName=String][FailureCause=String][FailureDetail=String][AppID=String][ClusterID=String][NodeID=String]: CAR scheduled job failed..

Explanation A normal CAR scheduled job failed for some reasons.

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.

Error Message

%UC_CAR-3-CARSchedulerJobInterrupted: %[JobName=String][FailureCause=String][FailureDetail=String][AppID=String][ClusterID=String][NodeID=String]: CAR scheduled job interrupted.

Explanation A normal CAR scheduled job interrupted for some reasons.

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.

Error Message

%UC_CAR-3-BadCDRFileFound: %[FileName=String][BadFileCause=String][BadFileSummary=String][AppID=String][ClusterID=String][NodeID=String]: Bad CDR or CMR flat file found during CDR Load to CAR database..

Explanation A bad CDR or CMR flat file is found during loading to CAR database, the file could be corrupted for some reasons. However, CAR loader is able to skip the bad record(s) and load the good ones to CAR database.

Recommended Action 1. Find the bad file from the cdr_repository folders, and check its problematic record(s) based on the information given by the cause and summary. 2. Collect the associated SDI and SDL traces for the bad record(s) found in this file as soon as possible. 3. Collect and check the CAR Scheduler traces for more details.

Error Message

%UC_CAR-7-CARIDSEngineDebug: %[Specific-Msg=String][ClassMsg=String][ClassID=String][AppID=String][ClusterID=String][NodeID=String]: Indicates debug events from CAR IDS database engine..

Explanation This alarm provides low-level debugging information from CAR IDS database engine. System administrator can disregard this alarm.

Recommended Action This is for debug information purposes only; no action is required.

Error Message

%UC_CAR-6-CARIDSEngineInformation: %[Specific-Msg=String][ClassMsg=String][ClassID=String][AppID=String][ClusterID=String][NodeID=String]: No error has occurred but some routine event

completed in CAR IDS database engine..

Explanation This alarm is informational. No error has occurred but some routine event completed in CAR IDS database engine.

Recommended Action This is for information purposes only; no action is required.

Error Message

%UC_CAR-2-CARIDSEngineCritical: %[Specific-Msg=String][ClassMsg=String][ClassID=String] [AppID=String][ClusterID=String][NodeID=String]: Pay Attention. This alarm does not compromise data or prevent the use of the system..

Explanation Pay Attention. This alarm does not compromise data or prevent the use of the system.

Recommended Action This alarm needs monitoring by the CAR DB admin.

Error Message

%UC_CAR-3-CARIDSEngineFailure: %[Specific-Msg=String][ClassMsg=String][ClassID=String] [AppID=String][ClusterID=String][NodeID=String]: Combined alarm for emergency and error situations. Something unexpected occurred that might compromise data or access to data or cause CAR IDS to fail..

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

Recommended Action Requires CAR DB admin intervention.

Error Message

%UC_CDP-2-DUPLEX_MISMATCH: %[SwitchDuplex=String][LocalInterfaceDuplex=String] [AppID=String][ClusterID=String][NodeID=String]: Duplex Mismatch Alarm.

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

Recommended Action Ensure that Duplex settings are set to auto or full on local inetrface as well as switch interface

Error Message

%UC_CAPF-0-CAPFCertificateKeyPairMismatch: %[AppID=String][ClusterID=String] [NodeID=String]: CAPF certificate is not have matching public- private key pair.

Explanation CAPF Service is not having matching certificate and key pair.

Recommended Action 1. Regenerate CAPF certificate. 2.Restart CAPF service. 3.Rerun CTLClient.4.Restart TFTP and Call Manager services.

Error Message

%UC_CAPF-6-CAPFCertificateRegenerated: %[AppID=String][ClusterID=String] [NodeID=String]: CAPF Service Restarted

Explanation CAPF Service is restarted due to the regeneration of the CAPF certificate.

Recommended Action Information purposes only; no action is required

Error Message

%UC_EXTENSIONMOBILITY-3-EMCCFailedInLocalCluster: %[DeviceName=String][TimeStamp=String] [UserID=String][Reason=String][AppID=String][ClusterID=String][NodeID=String]: EMCC Login failure in local Call Manager..

Explanation EMCC login could fail due to 1. Using devices incompatile with EMCC feature. 2. Unable to retrieve remote cluster information. 3. EMCC is restricted by the local cluster. 4. Untrusted Certificate received from the remote end while trying to establish a connection

Recommended Action 1. Validate if the device model supports EMCC (EMCC Documentation). 2. Ensure that every remote cluster added for EMCC has valid hostname/IP address(es) for EM and PSTN Access in the RemoteCluster administration page (Logon to CUCM Administration page -> System -> EMCC -> Remote Cluster). Also, ensure that these entries are enabled. 3. 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 -> Check the certificates in tomcat-trust).

Error Message

%UC_EXTENSIONMOBILITY-4-EMCCFailedInRemoteCluster: %[DeviceName=String] [TimeStamp=String][UserID=String][Reason=String][AppID=String][ClusterID=String] [NodeID=String]: EMCC Login failure at a remote Call Manager..

Explanation EMCC login could fail due to 1. User does not exist in any of the configured remote cluster. 2. User is not enabled for EMCC. 3. No free EMCC Base Device. 4. EMCC Access was prevented by remote cluster. 5. Untrusted Certificate received from the remote end while trying to establish a connection

Recommended Action 1. Ensure that the user is a valid EMCC user and make sure that user's home cluster is added as a EMCC remote cluster(Logon to CUCM Administration page -> System -> EMCC -> Remote Cluster -> Add New). 2. Contact remote site administrator to enable user for EMCC (Logon to CUCM Administration page -> User Management -> End User -> Select User -> Enable Extension mobility cross cluster checkbox) 3. Contact remote site administrator for adding / freeing up EMCC Base Devices (Logon to CUCM Administration page -> Bulk Administration -> EMCC -> Insert/Update EMCC). 4. Contact remote site administrator to validate the remote cluster setting for this cluster. 5. 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 -> Check for all tomcat certificates in tomcat-trust).

Error Message

%UC_EXTENSIONMOBILITY-4-UserInputFailure: %[DeviceName=String][TimeStamp=String] [UserID=String][Reason=String][AppID=String][ClusterID=String][NodeID=String]: EMCC Login failure due to invalid user input..

Explanation EMCC Login failed due to error in user input. This situation can arise due to 1. Invalid User Credentials. 2. Credentials have expired.

Recommended Action 1. Try again with valid credentials or try resetting the credentils.

Error Message

%UC_EXTENSIONMOBILITY-6-EMCCUserLoggedIn: %[DeviceName=String][TimeStamp=String] [UserID=String][AppID=String][ClusterID=String][NodeID=String]: EMCC login was successful..

Explanation The user has successfully logged in to extension mobility cross-cluster (EMCC).

Recommended Action Informational purposes only; no action is required.

Error Message

%UC_EXTENSIONMOBILITY-6-EMCCUserLoggedOut: %[DeviceName=String][TimeStamp=String] [UserID=String][AppID=String][ClusterID=String][NodeID=String]: EMCC logout was successful..

Explanation The user has successfully logged out of extension mobility cross-cluster (EMCC).

Recommended Action Informational purposes only; no action is required.

Error Message

%UC_EXTENSIONMOBILITY-6-EMAppStarted: %[ServletName=String][AppID=String] [ClusterID=String][NodeID=String]: EM Application started .

Explanation Application started successfully.

Recommended Action No action required.

Error Message

%UC_EXTENSIONMOBILITY-5-EMAppStopped: %[ServletName=String][AppID=String] [ClusterID=String][NodeID=String]: EM Application stopped.

Explanation Application is shutting down gracefully because of an unloaded from Tomcat.

Recommended Action No action required on this application.

Error Message

%UC_EXTENSIONMOBILITY-3-EMAppInitializationFailed: %[ServletName=String][AppID=String] [ClusterID=String][NodeID=String]: EM Application not started.

Explanation Error occurred while starting application.

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

Error Message

%UC_EXTENSIONMOBILITY-3-EMServiceConnectionError: %[ServletName=String][AppID=String] [ClusterID=String][NodeID=String]: EM Service not reachable.

Explanation EM Service might be down in one or more nodes in the cluster.

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

Error Message

%UC_EXTENSIONMOBILITY-3-NodeNotTrusted: %[TimeStamp=String][HostName=String] [AppID=String][ClusterID=String][NodeID=String]: Untrusted Node was contacted.

Explanation Application could not establish secure connection (SSL handshake failure) with another application. It could be due to 1. Certificate for tomcat service where the application is hosted is not trusted (not present in the keytore)

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).

Error Message

%UC_SYSAGENT-3-SyslogStringMatchFound: %[StringMatch=String][MatchedEvent=String] [AppID=String][ClusterID=String][NodeID=String]: The configured Syslog Alarm/message string had matched.

Explanation Cisco Syslog Agent had detected an alarm which matches the configured string

Recommended Action Take the necessary action based on the received string matched event

Error Message

%UC_SYSAGENT-3-HardwareFailure: %[hwStringMatch=String][AppID=String][ClusterID=String] [NodeID=String]: Hardware failure alarm is received.

Explanation Cisco Syslog Agent had detected a hardware failure alarm

Recommended Action Take the necessary action based on the received hardware failure event

Error Message

%UC_SYSAGENT-3-TCPRemoteSyslogDeliveryFailed: %[RemoteSyslogServerIP=String] [RecommendedTCPPort=String][Source=Enum][AppID=String][ClusterID=String] [NodeID=String]: Indicates a failure in delivering events to RemoteSyslogServer over TCP

Explanation This alarm indicates a failure occurred in delivering the events to the configured remote syslog server. The reason could be that the configured syslog server is down, or TCP is not configured to port 601, or there is a network failure.

Recommended Action Check that the configured remote syslog server is up, TCP protocol configured on the recommended port 601. If the issue persists, please contact Cisco Technical Assistance Center (TAC) for further support.

Error Message - Enum Definitions

Enum Definitions - Source

Value	Definition
0	Failure occurred while delivering alarm/audit events
1	Failure occurred while delivering Rsyslog generated

	events

Error Message

%UC_SYSAGENT-3- TLSRemoteSyslogDeliveryFailed : %[RemoteSyslogServerIP=String][RecommendedTLSPort =Int][Source=Enum][AppID=String][ClusterID=String][NodeID=String]: Indicates a failure in delivering events to RemoteSyslogServer over TLS

Explanation This alarm indicates a failure occurred in delivering the events to the configured remote syslog server. The reason could be that the configured syslog server is down, or TLS is not configured to port 6514, or there is a network failure, or certificate exchange between cucm and the remote syslog server might not have done.

Recommended Action Check that the configured remote syslog server is up, TLS protocol configured on the recommended port 6514 and proper certificate exchange is done between the cucm and remote syslog. If the issue persists, please contact Cisco Technical Assistance Center (TAC) for further support.

Error Message - Enum Definitions

Enum Definitions - Source

Value	Definition
0	Failure occurred while delivering alarm/audit events
1	Failure occurred while delivering Rsyslog generated events

Error Message

%UC_SYSAGENT-3-UnreachableRemoteSyslogServer: %[RemoteSyslogServerName=String] [ServiceName=String][AppID=String][ClusterID=String][NodeID=String]: The configured Remote syslog server is not reachable

Explanation This alarm indicates that the remote syslog server configured for a service is not reachable. The reason could be the IP address may be invalid, or the configured syslog server may be down, or UDP/TCP/TLS may not be configured to the ports 514/601/6514, or there is a network failure.

Recommended Action Check whether the configured remote syslog server is up and reachable from this server. Verify the the correct protocol is configured with the CLI command "utils remotesyslog show protocol". The system will automatically try to send new messages to the remote syslog server in one hour or when an admin saves the configuration again in Alarm Configuration GUI. If this issue persists, please contact Cisco Technical Assistance Center (TAC) for further support.

Error Message

%UC_SYSAGENT-3-SyslogSeverityMatchFound: %[SeverityMatch=String][MatchedEvent=String] [AppID=String][ClusterID=String][NodeID=String]: The configured Syslog Alarm/message severity had matched.

Explanation Cisco Syslog Agent had detected an alarm which matches the configured severity

Recommended Action Take the necessary action based on the received severity matched event

Error Message

%UC_TVS-1-SDIControlLayerFailed: %[Error=Int][Reason=String][AppID=String][ClusterID=String] [NodeID=String]: Failed to update trace logging or alarm subsystem for new settings..

Explanation This usually indicates a lack of system resources or a failure in database access by the trace logging or alarm subsystem.

Recommended Action In Cisco Unified Serviceability, enable Detailed level traces in the Trace Configuration window for TVS and Cisco Database Layer Monitor services. Also, use RTMT to look for error messages 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 TVS service and database trace files.

Error Message

%UC_TVS-3-ConfigThreadReadConfigurationFailed: %[AppID=String][ClusterID=String] [NodeID=String]: Failed to retrieve enterprise parameter values from database at TVS service startup..

Explanation This is usually caused by database access failure.

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

Error Message

%UC_TVS-1-ConfigThreadChangeNotifyServerSingleFailed: %[AppID=String][ClusterID=String] [NodeID=String]: Failed to allocate resources to handle configuration change notification from database..

Explanation This usually indicates a lack of memory when there is a system issue such as running out of resources.

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.

Error Message

%UC_TVS-6-ITLFileRegenerated: %[AppID=String][ClusterID=String][NodeID=String]: New ITL File has been generated..

Explanation This usually means that a new certificate related to ITLFile has been modified.

Recommended Action None.

Error Message

%UC_TVS-6-TVSCertificateRegenerated: %[AppID=String][ClusterID=String][NodeID=String]: TVS Server certificate has been regenerated..

Explanation This usually means that the TVS certificate has been regenerated. TVS server will automatically be restarted

Recommended Action None.

Error Message

%UC_TVS-6-RollBackToPre8.0Disabled: %[AppID=String][ClusterID=String][NodeID=String]: Roll Back to Pre 8.0 has been disabled in the Enterprise Parameter page..

Explanation This usually means that the RollBack to Pre 8.0 feature is modified in the Enterprise Parameter page

Recommended Action None.

Error Message

%UC_TVS-6-RollBackToPre8.0Enabled: %[AppID=String][ClusterID=String][NodeID=String]: Roll Back to Pre 8.0 has been enabled in the Enterprise Parameter page..

Explanation This usually means that the RollBack to Pre 8.0 feature is modified in the Enterprise Parameter page

Recommended Action None.

Error Message

%UC_TVS-6-DurationInCacheModified: %[AppID=String][ClusterID=String][NodeID=String]: Default Value of Certificate duration in cache is modified in the Service Parameter page.

Explanation This usually means that the Default Certificate duration in cache value is modified int the Service Parameter page

Recommended Action None.

Error Message

%UC_TVS-6-ClusterSecurityModeModified: %[AppID=String][ClusterID=String] [NodeID=String]: Cluster Security Mode is modified..

Explanation This usually means that the Cluster Security mode has been modified

Recommended Action None.

Error Message

%UC_TVS-1-TVSServerListenSetSockOptFailed: %[nError=Int][IPAddress=String][Port=Int] [AppID=String][ClusterID=String][NodeID=String]: Failed to increase the size of the network buffer for

receiving file requests..

Explanation This usually indicates a lack of memory when there is a system issue such as running out of resources.

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.

Error Message

%UC_TVS-1-TVSServerListenBindFailed: %[nError=Int][IPAddress=String][Port=Int][AppID=String] [ClusterID=String][NodeID=String]: Fail to connect to the network port through which file requests are received..

Explanation 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.

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).

Error Message

%UC_AUDITLOG-6-AdministrativeEvent: %[UserID=String][ClientAddress=String][Severity=String] [EventType=String][ResourceAccessed=String][EventStatus=String][AuditDetails=String] [ComponentID=String][CompulsoryEvent=String][AuditCategory=String][AppID=String] [ClusterID=String][NodeID=String]: Audit Event is generated by this application .

Explanation Failed to write into the primary file path.

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.

Error Message

%UC_AUDITLOG-6-SecurityEvent: %[UserID=String][ClientAddress=String][Severity=String] [EventType=String][ResourceAccessed=String][EventStatus=String][AuditDetails=String] [ComponentID=String][CompulsoryEvent=String][AuditCategory=String][AppID=String] [ClusterID=String][NodeID=String]: Audit Event is generated by this application .

Explanation Failed to write into the primary file path.

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.

Error Message

%UC_AUDITLOG-6-CriticalEvent: %[UserID=String][ClientAddress=String][Severity=String] [EventType=String][ResourceAccessed=String][EventStatus=String][AuditDetails=String]

[ComponentID=String][CompulsoryEvent=String][AuditCategory=String][AppID=String] [ClusterID=String][NodeID=String]: Audit Event is generated by this application .

Explanation Failed to write into the primary file path.

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.

Error Message

%UC_LOGIN-4-PlatformAdminAccountLocked: %[UserID=String][UnlockTime=String] [FailedLoginCount=String][AppID=String][ClusterID=String][NodeID=String]: A user attempted too many incorrect authentications and the corresponding account was locked by the platform.

Explanation A user repeatedly attempted to login using invalid credentials and the platform locked the user account when the user exhausted the number of allowed login attempts as specified by the FailedLoginCount shown in this alarm. The account remains locked until the number of seconds specified in the UnlockTime elapses.

Recommended Action Investigate why the user may have been attempting to login using invalid credentials to determine if the account lockout was the result of forgotten credentials or some other reason.

Error Message

%UC_FIPSMODECHANGEALARMCATALOG-5-FipsModeEnable: %[Message=String][AppID=String] [ClusterID=String][NodeID=String]: FIPS mode has been successfully enabled in the Cisco Unified Communications Manager. Certifcates for CUCM, CAPF, Tomcat, Ipsec , TVS and SSH services have been regenerated. .

Explanation This alarm is generated when the Cisco Unified Communications Manager OS administrator enables FIPS mode. Once FIPS mode has been enabled the system will reboot. After the reboot the system runs in compliance with the FIPS 140-2 Level 1 Standards.

Recommended Action The authorized administration should check all the FIPS logs to ensure that all FIPS related operations including the power up self tests completed successfully.

Error Message

%UC_FIPSMODECHANGEALARMCATALOG-5-FipsModeDisable: %[Message=String][AppID=String] [ClusterID=String][NodeID=String]: FIPS mode has been successfully disabled in the Cisco Unified Communications Manager. Certifcates for CUCM, CAPF, Tomcat, Ipsec , TVS and SSH services have been regenerated. .

Explanation This alarm is generated when the Cisco Unified Communications Manager OS administrator disables FIPS mode. Once FIPS mode has been disabledthe system will reboot.

Recommended Action The authorized administrator should check the FIPS logs to ensure there are no errors.

Error Message

%UC_ILS-3-ILSDBLException: %[DBLException=String][AppID=String][ClusterID=String] [NodeID=String]: An error occurred while the ILS was performing database activities.

Explanation A severe database layer interface error occurred. Some possible causes for this include the database being unreachable or down or a DNS error.

Recommended Action Review the System Reports provided in the Cisco Unified Reporting tool, specifically the Unified CM Database Status report, for any anomalous activity. 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. Check network connectivity to the server that is running the database. If your system uses DNS, check the DNS configuration for any errors. If the cause is still not identified, collect SDL and SDI traces and contact the Cisco Technical Assistance Center (TAC).

Error Message

%UC_ILS-3-ILSTLSAuthenticationFailed: %[Cluster1=String][AppID=String][ClusterID=String] [NodeID=String]: TLS authentication failure to cluster in this ILS network.

Explanation A TLS connection to a cluster in the ILS network could not be established, mostly likely because of a problem with the certificate presented by the publisher Unified CM in the remote cluster. (For example, not in the Unified CM CTL, or is in the CTL but has expired).

Recommended Action Verify that the certificate of the remote cluster Unified CM is installed and configured properly on the local Unified CM.

Error Message

%UC_ILS-3-ILSPwdAuthenticationFailed: %[IPAddress=String][AppID=String][ClusterID=String] [NodeID=String]: Password authentication failure to cluster in this ILS network.

Explanation A password authentication failure has occurred on a connection to a remote cluster.

Recommended Action Verify that ILS at the remote server is configured to use password authentication. Reenter the ILS password if needed. The ILS password must be identical at all clusters that will participate in the same ILS network.

Error Message

%UC_ILS-3-ILSDuplicateClusterID: %[EntClusterID=String][AppID=String][ClusterID=String] [NodeID=String]: Duplicate Enterprise Cluster ID found in ILS network.

Explanation A duplicate Enterprise Cluster ID has been found in this ILS network.

Recommended Action Check that the Enterprise Cluster ID is not set to the default value. Assign each cluster in the ILS network a unique Enterprise Cluster ID.

Error Message

%UC_ILS-3-ILSHubClusterUnreachable: %[HubCluster=String][ConnDetails=String][AppID=String] [ClusterID=String][NodeID=String]: Hub cluster unreachable..

Explanation This alarm indicates that the ILS was unable to reach the remote hub cluster. ILS will periodically re-attempt to connect to the hub cluster. If the condition is due to a temporary Internet connectivity issue, the problem will self-repair. However, if it is due to a persistent condition, action must be taken.

Recommended Action Make sure ILS is activated and running at the remote hub cluster. The hostname and IP address that ILS attempted connection to are included in the alarm. Verify that your firewall configuration is allowing the ILS access to the remote server. Try pinging the configured IP address of the remote server, and diagnose any network issues from there.

Error Message

%UC_ILS-2-ILSTCPInUse: %[PortNumber=UInt][AppID=String][ClusterID=String][NodeID=String]: ILS failed while initializing a TCP port because the port is already in use..

Explanation This alarm indicates that ILS was unable to bind to a TCP port because the port is already in use. It will occur during service startup if the ports that ILS tries to initialize are already in use. ILS will terminate when this error occurs.

Recommended Action Make sure that no other services have been configured to use the same ports that ILS has been configured to use. Correct the problem and restart ILS.

Error Message

%UC_ILS-2-ILSTCPListenError: %[PortNumber=UInt][AppID=String][ClusterID=String][NodeID=String]: ILS failed while initializing a TCP port..

Explanation This alarm indicates that ILS was unable to initialize a TCP port. It will occur during service startup when it tries to initialize TCP ports. ILS will terminate when this error occurs.

Recommended Action Consult the diagnostics for details.

Error Message

%UC_ILS-3-ILSRemoteHostUnresponsive: %[ClusterId=String][ConnectionDetail=String][AppID=String][ClusterID=String][NodeID=String]: No response from host at remote cluster..

Explanation ILS was able to establish a connection but the remote host was unresponsive. The connection has been dropped and ILS will periodically re-attempt to connect to remote cluster. If the condition is due to a temporary Internet connectivity issue, the problem will self-repair. However, if it is due to a persistent condition, action must be taken.

Recommended Action Verify the ILS configuration at the remote cluster. Check the remote cluster's syslog for additional details. Diagnose any network issues between the two IP addresses provided in the connection details of this alarm.

Error Message

%UC_ILS-3-ILSUnacceptableConnectionAttempt: %[Reason=String][ConnectionDetail=String][AppID=String][ClusterID=String][NodeID=String]: A connection from a remote ILS server has been rejected..

Explanation ILS received a connection attempt that was not acceptable. The connection has been dropped. Typically this alarm indicates a misconfiguration or incompatibility of ILS between the local and remote clusters.

Recommended Action Use the reason message provided to further diagnose the issue. The connection details will include the IP address of the remote ILS.

Error Message

%UC_ILS-3-ILSProtocolVersion: %[ClusterId=String][ConnectionDetail=String][AppID=String][ClusterID=String][NodeID=String]: Incompatible ILS protocol used by remote cluster..

Explanation ILS protocol used by remote system is not compatible with the local cluster. The connection has been dropped.

Recommended Action Upgrade the lower version component so that both clusters use the same or compatible version.

Error Message

%UC_ILS-4-ILSPeerLimitApproachingWarning: %[CurrentPeerCount=UInt][AppID=String] [ClusterID=String][NodeID=String]: The current peer count has reached 90% or more of the ILS network capacity(ILSP_MSG_PEER_MAX=200).

Explanation The current peer count has reached 90% or more of the ILS network capacity.

Recommended Action Make sure that the number of peers in the ILS network does not exceed 200.

Error Message

%UC_ILS-3-ILSPeerLimitExceeded: %[MaxPeerCount=UInt][AppID=String][ClusterID=String] [NodeID=String]: Exceeded maximum number of peers in ILS network(ILSP_MSG_PEER_MAX=200).

Explanation >The number of peers for this cluster in the ILS network is more than the limit set for ILSP_MSG_PEER_MAX. The system will be allowed to add spokes, hubs, and imported catalogs continuously; however, only max number of peers will be advertised to the ILS network.

Recommended Action Disconnect and rejoin the clusters to the ILS network to clean up obsoleted peers.

Error Message

%UC_Location Bandwidth Manager-2-LocationBandwidthManagerFailure: %[Text=String] [HostName=String][IPAddress=String][Reason=Enum][AppID=String][ClusterID=String] [NodeID=String]: Indicates an internal failure in LBM.

Explanation This alarm indicates that an internal failure occurred in the Cisco Location Bandwidth Manager Service. The service should restart in an attempt to clear the failure.

Recommended Action Monitor for other alarms and restart Cisco Location Bandwidth Manager Service, if necessary. Collect the core file if available, SDL and CCM/SDI trace files (you can gather these from Trace and Log Central in RTMT using the Collect Files feature) and contact the Cisco Technical Assistance Center (TAC).

Reason Code - Enum Definitions

Enum Definitions - Reason

Value	Definition
1	Unknown - LBM 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

Error Message

%UC_Location Bandwidth Manager-5-LBMLinkISV: %[RemoteIPAddress=String][LinkID=String] [LocalNodeId=UInt][LocalApplicationId=Enum][RemoteApplicationId=Enum][AppID=String] [ClusterID=String][NodeID=String]: LBM link to remote application restored.

Explanation This alarm indicates that the LBM has gained communication with the remote LBM. Note that the remote LBM should also indicate LBMLinkISV.

Recommended Action Informational only; no action is required

Reason Code - Enum Definitions

Enum Definitions - LocalApplicationId

Value	Definition
700	LocationBandwidthManager

Enum Definitions - RemoteApplicationId

Value	Definition
700	LocationBandwidthManager

Error Message

%UC_Location Bandwidth Manager-1-LBMLinkOOS: %[RemoteIPAddress=String][LinkID=String] [LocalNodeId=UInt][LocalApplicationID=Enum][RemoteNodeID=UInt][RemoteApplicationID=Enum] [AppID=String][ClusterID=String][NodeID=String]: LBM link to remote application is out of service.

Explanation This alarm indicates that the local LBM has lost communication with the remote LBM. 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).

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

Reason Code - Enum Definitions

Enum Definitions - LocalApplicationID

Value	Definition
700	LocationBandwidthManager

Enum Definitions - RemoteApplicationID

Value	Definition
700	LocationBandwidthManager

Error Message

%UC_Location Bandwidth Manager-1-LBMVersionMismatch: %[RemoteAppProtocolVersion=String] [LocalAppProtocolVersion=String][RemoteNodeId=UInt][RemoteAppId=Enum]

[RemoteAppVersion=String][AppID=String][ClusterID=String][NodeID=String]: One or more Unified LBM nodes in a cluster are running different LBM versions.

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

Recommended Action The alarm details include the versions of the local and remote LBM nodes. Compare the versions and upgrade the node if necessary.

Reason Code - Enum Definitions

Enum Definitions - RemoteAppId

Value	Definition
700	LocationBandwidthManager

Error Message

%UC_Location Bandwidth Manager-4-PrimaryHubUnreachable: %[LBMHubNode=String] [AppID=String][ClusterID=String][NodeID=String]: Primary LBM Hub Node Unreachable..

Explanation This alarm indicates that the LBM spoke node was unable to connect to Primary LBM Hub Node configured in LBM Hub Group table. The LBM Node will attempt to connect to Secondary and Tertiary LBM Hub Node. If the condition is due to a temporary Network connectivity issue, the problem will self-repair. However, if it is due to a persistent condition, action must be taken.

Recommended Action Make sure that your firewall configuration is allowing the LBM Node to access the Primary LBM Hub node. If firewall configurations are correct, try pinging the configured IP address and port of the Primary LBM Hub Node, and diagnose any network issues from there. The IP address and port of the Primary LBM Hub Node that was tried by the LBM Node is included as name/value pair in the alarm.

Error Message

%UC_Location Bandwidth Manager-4-SecondaryHubUnreachable: %[LBMHubNode=String] [AppID=String][ClusterID=String][NodeID=String]: Secondary LBM Hub Node Unreachable..

Explanation This alarm indicates that the LBM spoke node was unable to connect to Secondary LBM Hub Node configured in LBM Hub Group table. The LBM Node will attempt to connect back to Primary Hub Node.

Recommended Action No action is required on your part.

Error Message

%UC_Location Bandwidth Manager-4-TertiaryHubUnreachable: %[LBMHubNode=String] [AppID=String][ClusterID=String][NodeID=String]: Tertiary LBM Hub Node Unreachable..

Explanation This alarm indicates that the LBM spoke node was unable to connect to Tertiary LBM Hub Node configured in LBM Hub Group table. The LBM Node will attempt to connect back to Primary Hub Node.

Recommended Action No action is required on your part.

Error Message

%UC_Location Bandwidth Manager-2-LBMHubUnreachable: %[PrimHubNode=String] [SecondaryHubNode=String][TertiaryHubNode=String][AppID=String][ClusterID=String] [NodeID=String]: LBM Hub Nodes Unreachable..

Explanation This alarm indicates that the LBM spoke node was unable to connect to any of the LBM Hub Nodes configured in LBM Hub Group table. The LBM Spoke Node will periodically re-attempt to connect to the LBM Hub Nodes. If the condition is due to a temporary Network connectivity issue, the problem will self-repair. However, if it is due to a persistent condition, action must be taken.

Recommended Action Make sure that your firewall configuration is allowing the LBM Spoke Node to access the LBM Hub Nodes. If firewall configurations are correct, try pinging the configured IP addresses and ports of the LBM Hub Nodes, and diagnose any network issues from there. The IP addresses and ports of the LBM Hub Nodes that were tried by the LBM Spoke node are included as name/value pairs in the alarm.

Error Message

%UC_Location Bandwidth Manager-4-SuspiciousIPAddress: %[PortNumber=UInt][Address=String] [AppID=String][ClusterID=String][NodeID=String]: LBM has identified suspicious connection attempts from an IP address.

Explanation LBM has identified suspicious connection attempts from an IP address and has temporarily blocked the address. This alarm is an indication that a Denial-of-Service attack may have been attempted from this IP address.

Recommended Action Examine network activity for repeated attempts to access the port number specified in this alarm. Using the IP address specified in this alarm, attempt to identify the device that has been sending connection attempts to the port. If the IP address belongs to a device that is configured in IME, evaluate the possible reason for such numerous connection attempts. Generally, no device that is functioning properly will trigger this alarm. Reset the device or remove the device from the network.

Error Message

%UC_Location Bandwidth Manager-2-LBMServicePortFailedToOpen: %[Protocol=String] [PortNumber=UInt][ErrorNumber=Int][AppID=String][ClusterID=String][NodeID=String]: LBM service

port fails to be opened.

Explanation LBM socket port that is used to provide service fails to open.

Recommended Action Please check the LBM configuration to make sure that this port is not used by other applications. If this alarm occurs repeatly, collect the existing trace files and contact the Cisco Technical Assistance Center (TAC).

Error Message

%UC_Location Bandwidth Manager-4-LocationOutOfResource: %[Name=String] [ResourceType=Enum][AppID=String][ClusterID=String][NodeID=String]: All bandwidth allocated to the location/link is used up and no resources are available.

Explanation The Location or Link connecting locations has run out of audio/video/immersive bandwidth and hence no further calls can originate or pass through the location/link. The out of resource condition may be temporary due to high number of calls during peak hours and may correct by itself when calls terminate and bandwidth is freed up.

Recommended Action Consider adding additional bandwidth to the location/link.

Reason Code - Enum Definitions

Enum Definitions - ResourceType

Value	Definition
1	Audio bandwidth out of resource
2	Video bandwidth out of resource
3	Immersive bandwidth out of resource

Error Message

%UC_Location Bandwidth Manager-3-NoSuchLocation: %[Location=String][FullKey=String] [LocalNodeId=UInt][LocalApplicationId=Enum][AppID=String][ClusterID=String][NodeID=String]: A location name is unknown to the LBM service..

Explanation No such location exists or is recognized by LBM service.

Recommended Action Check whether the device supports assignment to the location (Shadow and Phantom are special). If the location is defined in a remote cluster, check the connectivity to that cluster ; check whether LBM services in the remote cluster are active; check LBM security mode mismatch between clusters; log off and log back in if this is an EMCC device.

Reason Code - Enum Definitions

Enum Definitions - LocalApplicationId

Value	Definition
700	LocationBandwidthManager

Error Message

%UC_Location Bandwidth Manager-3-NoPathExists: %[Location1=String][Location2=String] [FullKey=String][LocalNodeId=UInt][LocalApplicationId=Enum][AppID=String][ClusterID=String]

[NodeID=String]: A LBM service determined that no path exists between location 1 and location 2..

Explanation Location 1 and Location 2 are not connected.

Recommended Action Check whether the two locations are connected. If locations and/or links are defined in different clusters, check the connectivity to these clusters; check whether LBM services in all the affected remote clusters are active; check LBM security mode mismatch between clusters; log off and log back in if this is an EMCC device.

Reason Code - Enum Definitions

Enum Definitions - LocalApplicationId

Value	Definition
700	LocationBandwidthManager

Error Message

%UC_Location Bandwidth Manager-5-LBMRemoteHubNoSecureConnectionAlarm: %[RemoteIPAddress=String][LocalNodeId=UInt][LocalApplicationID=Enum][RemoteApplicationID=Enum][AppID=String][ClusterID=String][NodeID=String]: Lost LBM secure connection to remote LBM application.

Explanation This alarm indicates that the local LBM has lost secure communication with the remote LBM. 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); networking issues; or certificate issues.

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

Reason Code - Enum Definitions

Enum Definitions - LocalApplicationID

Value	Definition
700	LocationBandwidthManager

Enum Definitions - RemoteApplicationID

Value	Definition
700	LocationBandwidthManager

Error Message

%UC_Location Bandwidth Manager-5-LBMRemoteHubSecureConnectionRestoredAlarm: %[RemoteIPAddress=String][LocalNodeId=UInt][LocalApplicationId=Enum][RemoteApplicationId=Enum]

[AppID=String][ClusterID=String][NodeID=String]: Restored LBM secure connection to remote LBM application.

Explanation This alarm indicates that the LBM has gained secure communication with the remote LBM. Note that the remote LBM should also indicate LBMRemoteHubSecureConnectionAlarm.

Recommended Action Informational only; no action is required

Reason Code - Enum Definitions

Enum Definitions - LocalApplicationId

Value	Definition
700	LocationBandwidthManager

Enum Definitions - RemoteApplicationId

Value	Definition
700	LocationBandwidthManager

Error Message

%UC_Location Bandwidth Manager-5-LBMRemoteHubNoInsecureConnectionAlarm: %[RemoteIPAddress=String][LocalNodeId=UInt][LocalApplicationID=Enum][RemoteApplicationID=Enum][AppID=String][ClusterID=String][NodeID=String]: Lost LBM insecure connection to the remote LBM application.

Explanation This alarm indicates that the local LBM has lost insecure communication with the remote LBM. 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).

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

Reason Code - Enum Definitions

Enum Definitions - LocalApplicationID

Value	Definition
700	LocationBandwidthManager

Enum Definitions - RemoteApplicationID

Value	Definition
700	LocationBandwidthManager

Error Message

%UC_Location Bandwidth Manager-5-LBMRemoteHubInsecureConnectionRestoredAlarm: %[RemoteIPAddress=String][LocalNodeId=UInt][LocalApplicationId=Enum][RemoteApplicationId=Enum][AppID=String][ClusterID=String][NodeID=String]: Restored LBM insecure connection to remote LBM.

Explanation This alarm indicates that the LBM has gained secure communication with the remote LBM. Note that the remote LBM should also indicate LBMRemoteHubSecureConnectionAlarm.

Recommended Action Informational only; no action is required

Reason Code - Enum Definitions

Enum Definitions - LocalApplicationId

Value	Definition
700	LocationBandwidthManager

Enum Definitions - RemoteApplicationId

Value	Definition
700	LocationBandwidthManager

Error Message

%UC_Location Bandwidth Manager-3-LBMRemoteHubNoConnectionAlarm: %[RemoteIPAddress=String][LocalNodeId=UInt][LocalApplicationID=Enum][RemoteApplicationID=Enum][AppID=String][ClusterID=String][NodeID=String]: Lost LBM all connection to the remote LBM application.

Explanation This alarm indicates that the local LBM has lost all communications with the remote LBM. 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).

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

Reason Code - Enum Definitions

Enum Definitions - LocalApplicationID

Value	Definition
700	LocationBandwidthManager

Enum Definitions - RemoteApplicationID

Value	Definition
700	LocationBandwidthManager

Error Message

%UC_Location Bandwidth Manager-5-LBMRemoteHubConnectionRestoredAlarm: %[RemoteIPAddress=String][LocalNodeId=UInt][LocalApplicationId=Enum][RemoteApplicationId=Enum]

[AppID=String][ClusterID=String][NodeID=String]: Restored LBM connection to remote LBM application.

Explanation This alarm indicates that the LBM has gained secure communication with the remote LBM. Note that the remote LBM should also indicate LBMRemoteHubSecureConnectionAlarm.

Recommended Action Informational only; no action is required

Reason Code - Enum Definitions

Enum Definitions - LocalApplicationId

Value	Definition
700	LocationBandwidthManager

Enum Definitions - RemoteApplicationId

Value	Definition
700	LocationBandwidthManager

Explanation This alarm indicates that the LBM has gained secure communication with the remote LBM. Note that the remote LBM should also indicate LBMRemoteHubSecureConnectionAlarm.

Recommended Action Informational only; no action is required

Error Message

%UC_ICSA-2-InterclusterSyncAgentPeerDuplicate: %[hostname=String][existingPeer=String] [AppID=String][ClusterID=String][NodeID=String]: Cisco Intercluster Sync Agent service failed to sync with remote peer.

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

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

Error Message

%UC_ICSA-2-ICSACertificateFingerPrintMisMatch: %[SubjectCN=String][IssuerCN=String] [AppID=String][ClusterID=String][NodeID=String]: Cisco Intercluster Sync Agent service detected a fingerprint mismatch on the certificate being processed.

Explanation Cisco Intercluster Sync Agent service detected a fingerprint mismatch on the certificate being processed

Recommended Action Use the IM and Presence Service Platform GUI to compare the certificates loaded on this server with the certificates on the source server. It may necessary to delete the problem certificates and reload them

Error Message

%UC_ICSA-2-ICSACertificateValidationFailure: %[SubjectCN=String][IssuerCN=String] [ErrorCode=String][AppID=String][ClusterID=String][NodeID=String]: Cisco Intercluster Sync Agent service detected a validation error on the certificate being processed.

Explanation Cisco Intercluster Sync Agent service detected a validation error on the certificate being processed

Recommended Action Use the IM and Presence Service Platform GUI to compare the certificates loaded on this server with the certificates on the source server. It may necessary to delete the problem certificates and reload them

Error Message

%UC_ICSA-4-ICSACertificateCAConflict: %[SubjectCN=String][IssuerCN=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco Intercluster Sync Agent service detected a CA certificate conflict

Explanation Cisco Intercluster Sync Agent service detected a CA certificate conflict

Recommended Action A conflicting CA certificate was detected on CUCM when auditing certificates. Stop the Cisco Intercluster Sync Agent on all IM and Presence nodes in the cluster. Delete the conflicting certificate on all CUCM and IM and Presence nodes and re-upload the valid certificate to each node. Start the Cisco Intercluster Sync Agent

Error Message

%UC_ICSA-2-InterClusterSyncAgentPeerSyncFailure: %[remotePeerAddress=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco Intercluster Sync Agent service detected periodic sync failure

Explanation Cisco Intercluster Sync Agent is unable to read the remote peer's hostname or IP address of the IM and Presence node. The service will try resyncing every 5 minutes.

Recommended Action Verify that the hostname or IP address of the IM and Presence node is present in System -> Server configuration page on remote cluster's Cisco Unified CM Administration.

Error Message

%UC_ICSA-2-InterClusterSyncAgentDomainConflict: %[remotePeerAddress=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco Intercluster Sync Agent service detected periodic sync failure

Explanation Cisco Intercluster Sync Agent detected proxy domains mismatch. The service will try resyncing every 30 minutes

Recommended Action Cisco Intercluster Sync Agent detected proxy domains mismatch. The service will try resyncing every 30 minutes

Error Message

%UC_ICSA-2-InterClusterSyncAgentSyncFailure: %[remotePeerAddress=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco Intercluster Sync Agent service detected periodic sync failure

Explanation Cisco Intercluster Sync Agent service detected an exception.

Recommended Action Cisco Intercluster Sync Agent service will try resyncing every 5 minutes.

Error Message

%UC_ICSA-6-InterClusterSyncAgentAxlClientTimeout: %[remotePeerAddress=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco Intercluster Sync Agent service detected periodic sync failure

Explanation Cisco Intercluster Sync Agent service could not establish an AXL connection with the remote peer. The service will try resyncing every 5 minutes.

Recommended Action Verify that the Cisco AXL Web Service on the remote peer is running.

Error Message

%UC_ICSA-2-InterClusterSyncAgentHeapSpaceError: %[AppID=String][ClusterID=String] [NodeID=String]: Cisco Intercluster Sync Agent service detected a heap space error

Explanation Cisco Intercluster Sync Agent service detected a heap space error.

Recommended Action Restart Cisco Intercluster Sync Agent service.

Error Message

%UC_ICSA-6-InterClusterSyncAgentStatus: %[remotePeerAddress=String][AppID=String] [ClusterID=String][NodeID=String]: Periodic sync completed successfully

Explanation Periodic sync completed successfully for remote peer.

Recommended Action Informational purposes only; no action is required.

Error Message

%UC_ICSA-6-InterClusterSyncAgentControllerStatus: %[remotePeerAddress=String][AppID=String] [ClusterID=String][NodeID=String]: Peer sync controller created successfully

Explanation Peer sync controller created successfully for remote peer.

Recommended Action Informational purposes only; no action is required.

Error Message

%UC_ICSA-2-InterClusterSyncAgentPeerPeriodicSyncingFailure: %[remotePeerAddress=String] [lastSynchronizedTime=String][AppID=String][ClusterID=String][NodeID=String]: Cisco Intercluster Sync Agent service detected periodic syncing failure with an inter-cluster peer

Explanation Cisco Intercluster Sync Agent service detected a failure for the periodic syncing. It will try to recover the periodic syncing automatically if the Service Parameter "Enable Auto Recovery for Inter-cluster Peer Periodic Syncing Failure" of Inter-Cluster Sync Agent service is enabled.

Recommended Action Cisco Intercluster Sync Agent service detected a failure for the periodic syncing. It will try to recover the periodic syncing automatically if the Service Parameter "Enable Auto Recovery for Inter-cluster Peer Periodic Syncing Failure" of Inter-Cluster Sync Agent service is enabled.

Error Message

%UC_ICSA-2-InterclusterSyncAgentPeerDown: %[remotePeer=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco Intercluster Sync Agent service has detected an Intercluster Peer is unreachable

Explanation Cisco Intercluster Sync Agent service detected remotePeer is unreachable via ping on TCP port 8443.

Recommended Action Verify the node remotePeer is up and the network connectivity from this node to remotePeer is reachable

Error Message

%UC_ICSA-2-MAencryptionMultiMaster: %[remotePeerAddress=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco Intercluster Sync Agent detected multi-master configuration

Explanation An ICSA Peer cluster is configured for encrypted message archiving with a different master from the local cluster.

Recommended Action Encrypted message archiving requires a single master cluster for all ICSA peers. To resolve this condition you must download the encryption key from the remote cluster and disable encrypted message archiving before adding the remote cluster(s) as ICSA Peers with this cluster.

Error Message

%UC_ICSA-3-InterClusterSyncAgentAppUserEndUserConflict: %[remotePeerAddress=String] [conflictingUserID=String][AppID=String][ClusterID=String][NodeID=String]: Cisco Intercluster Sync Agent service detected an End User on a peer cluster with a User ID that conflicts with an existing local Application User.

Explanation The peer End User with the conflicting User ID cannot be synced to this cluster because an Application User with the same User ID exists.

Recommended Action Rename the local Application User to allow the remote End User to be synced to this cluster.

Error Message

%UC_null-2-LocationServiceMseDown: %[hostname=String][AppID=String][ClusterID=String] [NodeID=String]: Cisco Location Service MSE Down Alarm.

Explanation MSE is down. Location services for this MSE will be unavailable.

Recommended Action Check IM/P Service logs and MSE logs to determine problem. After resolving issue, delete and re-add the MSE.

Error Message

%UC_ReplWatcher-4-ReplicationFailure: %[HostName=String][AppID=String][ClusterID=String] [NodeID=String]: Cisco IM and Presence Data Monitor detected replication failure.

Explanation Cisco IM and Presence Data Monitor has detected database replication failure on this node. If this node is currently starting, some services will be prevented from starting until replication is established.

Recommended Action Please check Cisco IM and Presence Data Monitor logs for details. Replication status can be manually checked via the command line interface.

Error Message

%UC_ReplWatcher-6-ReplicationFailureClear: %[HostName=String][AppID=String][ClusterID=String][NodeID=String]: Cisco IM and Presence Data Monitor detected that replication has been successfully established on this node..

Explanation Cisco IM and Presence Data Monitor has detected that replication has been successfully established on this node.

Recommended Action No action required. See Cisco IM and Presence Data Monitor logs for details.

Error Message

%UC_ReplWatcher-4-ReplicationFailureTimeout: %[HostName=String][AppID=String][ClusterID=String][NodeID=String]: Cisco IM and Presence Data Monitor startup timeout. Cisco IM and Presence Data Monitor is allowing services to continue startup although replication has not completed setup on this publisher node..

Explanation Cisco IM and Presence Data Monitor startup timeout. Cisco IM and Presence Data Monitor is allowing services to continue startup although replication has not completed setup on this publisher node.

Recommended Action Please check Cisco IM and Presence Data Monitor logs for details. Replication status can be manually checked via the command line interface.

Error Message

%UC_ReplWatcher-1-ReplicationIMAddressSchemeChangeFailure: %[HostName=String][AppID=String][ClusterID=String][NodeID=String]: Cisco IM and Presence Data Monitor has detected the database job to change the IM Address Scheme has failed..

Explanation Cisco IM and Presence Data Monitor has detected the database job to change the IM Address Scheme has failed. Cisco IM and Presence Data Monitor has stopped services.

Recommended Action Please rerun the IM Address Scheme change procedure from the Advanced Presence Settings page.

Error Message

%UC_ReplWatcher-1-ReplicationDefaultIMDomainChangeFailure: %[HostName=String][AppID=String][ClusterID=String][NodeID=String]: Cisco IM and Presence Data Monitor has detected database job to change the local default IM domain has failed..

Explanation Cisco IM and Presence Data Monitor has detected the database job to change the local default IM domain has failed. Cisco IM and Presence Data Monitor has stopped services.

Recommended Action Please rerun the default IM domain change procedure from the Advanced Presence Settings page.

Error Message

%UC_ReplWatcher-1-DuplicateUserid: %[HostName=String][AppID=String][ClusterID=String][NodeID=String]: Cisco IM and Presence Data Monitor has detected that two or more users on the system share the same UserID value..

Explanation Cisco IM and Presence Data Monitor has detected that two or more users on the system share the same UserID value. This is a misconfiguration as all users must have a unique UserID. This may result in undetermined behaviour in routing IM and Presence packets to the affected users. It is

not possible for two users on the same cluster to share a common userID, so the conflicting users must reside on separate clusters.

Recommended Action Begin by compiling a list of the duplicate UserIDs. The User Troubleshooter section on the IM and Presence System Troubleshooter will display up to 10 duplicate UserIDs. Alternatively, the following Administration CLI command will supply all affected UserIDs: utils users validate. Once the list has been compiled, check to see why each UserID is being duplicated and take the appropriate action. There are two potential reasons why an entry may be marked as Duplicate. (1) The same user has been enabled for IM and Presence on more than one cluster. In this case, disable IM and Presence for the user for all but one of the clusters to solve the issue. (2) Two or more different users, each on different clusters share a common UserID. In this case, re-configure the appropriate user's UserIDs on CUCM such that they no longer conflict with one another. If UserID values are synced from a LDAP Directory, the reconfiguration may need to take place on that Directory.

Error Message

%UC_ReplWatcher-1-DuplicateDirectoryURI: %[HostName=String][AppID=String][ClusterID=String][NodeID=String]: Cisco IM and Presence Data Monitor has detected that two or more users on the system share the same Directory URI value..

Explanation Cisco IM and Presence Data Monitor has detected that two or more users on the system share the same Directory URI value. This is a misconfiguration as all users must have a unique Directory URI. This may result in undetermined behaviour in routing IM and Presence packets to the affected users. It is not possible for two users on the same cluster to share a common Directory URI, so the conflicting users must reside on separate clusters.

Recommended Action Begin by compiling a list of the duplicate Directory URIs. The User Troubleshooter section on the IM and Presence System Troubleshooter will display up to 10 duplicate Directory URIs. Alternatively, the following Administration CLI command will supply all affected Directory URIs: utils users validate. Once the list has been compiled, check to see why each URI is being duplicated and take the appropriate action. There are two potential reasons why an entry may be marked as Duplicate. (1) The same user has been enabled for IM and Presence on more than one cluster. In this case, disable IM and Presence for the user for all but one of the clusters to solve the issue. (2) Two or more different users, each on different clusters share a common DirectoryURI. In this case, re-configure the appropriate user's Directory URI on CUCM such that they no longer conflict with one another. If Directory URI values are synced from a LDAP Directory, the reconfiguration may need to take place on that Directory.

Error Message

%UC_ReplWatcher-4-DuplicateDirectoryURIWarning: %[HostName=String][AppID=String][ClusterID=String][NodeID=String]: Cisco IM and Presence Data Monitor has detected that two or more users on the system share the same Directory URI value..

Explanation Cisco IM and Presence Data Monitor has detected that two or more users on the system share the same Directory URI value. This is a misconfiguration as all users must have a unique Directory URI. This misconfiguration will not immediately impact users. However if the IM Addressing Scheme is switched to Directory URI, it will result in undetermined behaviour in routing IM and Presence packets to the affected users. It is not possible for two users on the same cluster to share a common Directory URI, so the conflicting users must reside on separate clusters.

Recommended Action Begin by compiling a list of the duplicate Directory URIs. The User Troubleshooter section on the IM and Presence System Troubleshooter will display up to 10 affected Directory URIs. Alternatively, the following Administration CLI command will supply all affected Directory URIs: utils users validate. Once the list has been compiled, check to see why each URI is being duplicated and take the appropriate action. There are two potential reasons why an entry may

be marked as Duplicate: 1) The same user has been enabled for IM and Presence on more than one cluster. In this case, disable IM and Presence for the user for all but one of the clusters to solve the issue. 2) Two or more different users, each on different clusters share a common DirectoryURI. In this case, re-configure the user's Directory URI on CUCM such that they no longer conflict with one another. If Directory URI values are synced from a LDAP Directory, the reconfiguration may need to take place on that Directory.

Error Message

%UC_ReplWatcher-1-InvalidDirectoryURI: %[HostName=String][AppID=String][ClusterID=String][NodeID=String]: Cisco IM and Presence Data Monitor has detected that one or more users have an invalid Directory URI value..

Explanation Cisco IM and Presence Data Monitor has detected that one or more users have an invalid Directory URI value. An invalid Directory URI is deemed an entry that is either empty or does not follow the basic user@domain URI format. This misconfiguration will mean the affected users will be unable to sign into IM and Presence.

Recommended Action Begin by compiling a list of the affected users. The User Troubleshooter section on the IM and Presence System Troubleshooter will display up to 10 affected users. Alternatively, the following Administration CLI command will supply all affected users and their home location: utils users validate. Once the list has been compiled, proceed to edit the Directory URI value for these users on CUCM. If the Directory URI field is synced from a LDAP Directory, make the required modification to that user on the Directory instead.

Error Message

%UC_ReplWatcher-4-InvalidDirectoryURIWarning: %[HostName=String][AppID=String][ClusterID=String][NodeID=String]: Cisco IM and Presence Data Monitor has detected that one or more users have an invalid Directory URI value..

Explanation Cisco IM and Presence Data Monitor has detected that one or more users have an invalid Directory URI value. An invalid Directory URI is deemed an entry that is either empty or does not follow the basic user@domain URI format. This misconfiguration will not immediately impact users. However if the IM Addressing Scheme is switched to Directory URI, the affected users will be unable to sign into IM and Presence.

Recommended Action Begin by compiling a list of the affected users. The User Troubleshooter section on the IM and Presence System Troubleshooter will display up to 10 affected users. Alternatively, the following Administration CLI command will supply all affected users and their home location: utils users validate. Once the list has been compiled, proceed to edit the Directory URI value for these users on CUCM. If the Directory URI field is synced from a LDAP Directory, make the required modification to that user on the Directory instead.

Error Message

%UC_ConfigAgent-3-EspConfigAgentMemAllocError: %[Location=String][AppID=String][ClusterID=String][NodeID=String]: Cisco Config Agent service was unable to allocate memory.

Explanation Cisco Config Agent service failed to allocate memory

Recommended Action Using RTMT, verify system memory is low or exhausted. This alarm may indicate the system is overloaded which may require reassigning users to other nodes in the IM and Presence Service cluster. You can reassign users to other nodes using the Topology page on the IM and Presence Service Administration GUI

Error Message

%UC_ConfigAgent-3-EspConfigAgentFileWriteError: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: Cisco Config Agent service was unable to write to the filesystem.

Explanation Cisco Config Agent service failed to write to a file. This may indicate the system is out of memory

Recommended Action Using RTMT, verify disk space is low or exhausted. This alarm may indicate the system is overloaded which may require reassigning users to other nodes in the IM and Presence Service cluster. You can reassign users to other nodes using the Topology page on the IM and Presence Service Administration GUI

Error Message

%UC_ConfigAgent-3-EspConfigAgentSharedMemoryStaticRouteError: %[AppID=String][ClusterID=String][NodeID=String]: Cisco Config Agent service could not access static route shared memory.

Explanation Cisco Config Agent service failed to access static routes in shared memory. This may indicate the system is out of memory

Recommended Action Using RTMT, verify system shared memory is low or exhausted. This alarm may indicate the system is overloaded which may require reassigning users to other nodes in the IM and Presence Service cluster. You can reassign users to other nodes using the Topology page on the IM and Presence Service Administration GUI

Error Message

%UC_ConfigAgent-5-EspConfigAgentServiceStartFailed: %[AppID=String][ClusterID=String][NodeID=String]: Cisco Config Agent failed to start a feature service.

Explanation Cisco Config Agent failed to start one of the feature services

Recommended Action Please use the serviceability page to check status and start the service manually

Error Message

%UC_ConfigAgent-5-EspConfigAgentServiceStopFailed: %[AppID=String][ClusterID=String][NodeID=String]: Cisco Config Agent failed to stop a feature service.

Explanation Cisco Config Agent failed to stop one of the feature services

Recommended Action Please use the serviceability page to check status and stop the service manually

Error Message

%UC_ConfigAgent-4-EspConfigAgentNetworkOutage: %[AppID=String][ClusterID=String] [NodeID=String]: Cisco Config Agent network outage.

Explanation Cisco Config Agent noticed a network outage

Recommended Action Using RTMT, verify system health and network connectivity.

Error Message

%UC_ConfigAgent-4-EspConfigAgentNetworkRestored: %[AppID=String][ClusterID=String] [NodeID=String]: Cisco Config Agent network restored.

Explanation Cisco Config Agent noticed network was restored

Recommended Action Using RTMT, verify system health and network connectivity.

Error Message

%UC_ConfigAgent-4-EspConfigAgentHighMemoryUtilization: %[AppID=String][ClusterID=String] [NodeID=String]: Virtual memory utilization has exceeded the configured threshold.

Explanation Available free virtual memory is low

Recommended Action Use RTMT to monitor memory use and reduce system load to improve performance if necessary. The memory watermark can be configured through the IM and Presence Service Administration GUI Service Parameters for the Cisco Config Agent

Error Message

%UC_ConfigAgent-5-EspConfigAgentHighMemoryUtilizationClear: %[AppID=String][ClusterID=String] [NodeID=String]: Virtual memory utilization is below the configured low watermark.

Explanation Virtual memory use exceeded the high memory use watermark, but has since fallen below the low memory watermark

Recommended Action Notification purposes only; no action is required

Error Message

%UC_ConfigAgent-4-EspConfigAgentHighCPUUtilization: %[AppID=String][ClusterID=String] [NodeID=String]: CPU utilization has exceeded the configured threshold.

Explanation CPU use is high

Recommended Action Use RTMT to monitor CPU use and reduce system load to improve performance if necessary. The CPU watermark can be configured through the IM and Presence Service Administration GUI Service Parameters for the Cisco Config Agent

Error Message

%UC_ConfigAgent-5-EspConfigAgentHighCPUUtilizationClear: %[AppID=String][ClusterID=String] [NodeID=String]: CPU utilization is below the configured low watermark.

Explanation CPU use exceeded the high CPU use watermark, but has since fallen below the low CPU watermark

Recommended Action Notification purposes only; no action is required

Error Message

%UC_ConfigAgent-3-EspConfigAgentLocalDBAccessError: %[AppID=String][ClusterID=String] [NodeID=String]: Cisco Config Agent service was unable to access the local IM and Presence Service

database.

Explanation Cisco Config Agent service failed to read or write to the local IM and Presence Service database. This may indicate a DB health issue.

Recommended Action Using RTMT, verify system health. Verify that the service "A Cisco DB" is running.

Error Message

%UC_ConfigAgent-4-EspConfigAgentRemoteDBAccessError: %[AppID=String][ClusterID=String][NodeID=String]: Cisco Config Agent service was unable to access a remote IM and Presence Service database.

Explanation Cisco Config Agent service failed to read or write to a remote IM and Presence Service database in the local cluster. This may indicate the system a DB health issue.

Recommended Action Verify that the service "A Cisco DB" is running on the node specified in the alert. Sometimes these errors can be transient. In some cases the Config Agent may be accessing remote nodes that are not available for some reason. If that is the case then this error is expected. This would happen in a user reassignment to a node that is not installed or available.

Error Message

%UC_ConfigAgent-4-EspConfigAgentProxyDomainNotConfigured: %[AppID=String][ClusterID=String][NodeID=String]: Cisco Config Agent service requires that the Default IM Domain is configured..

Explanation Cisco Config Agent service uses the Default IM Domain to properly generate ACLs. If not configured this could lead to routing failures.

Recommended Action Go to the Presence -> Settings -> Advanced Configuration Page on your IM and Presence Server to set this value and save.

Error Message

%UC_PE-2-PEDatabaseError: %[PEDatabaseErrorAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: Information lookup failed.

Explanation An error occurred while retrieving information. This may indicate a problem with the Cisco DB service

Recommended Action Verify that the Cisco DB service is activated and running. Use RTMT to check the Cisco Presence service logs for errors

Error Message

%UC_PE-2-PEPeerNodeFailure: %[PEPeerNodeFailureAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: The Cisco Presence Engine service on the peer node of a subcluster has failed.

Explanation The Cisco Presence Engine service in the peer node is not responding

Recommended Action Use Cisco Unified Serviceability to verify the Cisco Presence Engine service is activated and running

Error Message

%UC_PE-3-PEAutoRecoveryFailed: %[PEAutorecoveryFailedAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: Cisco Presence Engine service auto-recovery failure.

Explanation An error occurred during the startup sequence of the Cisco Presence Engine service

Recommended Action This error may indicate a possible configuration issue. Please correct the problem identified in the failure message

Error Message

%UC_PE-5-PEPeerNodeFailureCleared: %[PEPeerNodeFailureClearedAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: Cisco Presence Engine service on the clusters peer node has returned to normal operation.

Explanation The Cisco Presence Engine service running on the cluster peer node has returned to normal operation

Recommended Action Notification purposes only; no action is required

Error Message

%UC_PE-4-PELoadHighWaterMark: %[PELoadHighWaterMarkAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: Indicates the Cisco Presence Engine service has exceeded a CPU utilization threshold.

Explanation The Cisco Presence Engine service has detected that the CPU utilization has exceeded the configured threshold. During this time the Cisco Presence Engine service will reject/redirect SIP SUBSCRIBE requests until the CPU utilization drops below the configured threshold

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

Error Message

%UC_PE-5-PELoadHighWaterMarkCleared: %[PELoadHighWaterMarkClearedAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: Cisco Presence Engine service high water threshold has cleared.

Explanation The Cisco Presence Engine service has cleared the previous high water threshold (which was caused by high CPU utilization), and is now accepting SIP requests

Recommended Action Notification purposes only; no action is required

Error Message

%UC_PE-2-PEIDStoIMDBDatabaseSyncError: %[PEIDStoIMDBDatabaseSyncErrorAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: Synchronization between the IM and Presence Service Database and the Cisco Presence Engine database has failed.

Explanation An error has occurred synchronizing the IM and Presence Service data with the Cisco Presence Engine database

Recommended Action See associated error message and log files. Please restart the Cisco Presence Engine service when convenient

Error Message

%UC_PE-5-PEIDStoIMDBDatabaseSyncErrorCleared: %[PEIDStoIMDBDatabaseSyncErrorClearedAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: Synchronization between the IM and Presence Service database and the Cisco Presence Engine database established.

Explanation The Cisco Presence Engine service has established synchronization between IM and Presence Service database and the Cisco Presence Engine database

Recommended Action Notification purposes only; no action is required

Error Message

%UC_PE-2-PEIDSSubscribeError: %[PEIDSSubscribeErrorAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: The Cisco Presence Engine service was unable to subscribe for IM and Presence Service database change notifications.

Explanation An error has occurred subscribing to IM and Presence Service database change notifications

Recommended Action See associated error message and log files. Please restart the Cisco Presence Engine service when convenient

Error Message

%UC_PE-2-PEIDSQueryError: %[PEIDSQueryErrorAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: The Cisco Presence Engine service has detected an error while querying the IM and Presence Service database.

Explanation An error has occurred whilst querying the IM and Presence Service database

Recommended Action See associated error message and log files. Please restart the Cisco Presence Engine service when convenient

Error Message

%UC_PE-4-PEMemoryHigh: %[PEMemoryHighAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: Indicates the Cisco Presence Engine service has hit a high memory threshold.

Explanation The Cisco Presence Engine service has encountered a high memory condition. The Cisco Presence Engine service will reject or redirect SIP SUBSCRIBE requests until the memory condition has cleared

Recommended Action Inspect the number of active subscription counters: ActiveSubscriptions, ActiveViews, SubscriptionActiveReceivedFromForeign and SubscriptionActiveSentForeign with RTMT. If this condition occurs consistently, consider offloading some users to a different IM and Presence node in the cluster

Error Message

%UC_PE-5-PEMemoryHighCleared: %[PEMemoryHighClearedAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: Indicates that the Cisco Presence Engine service has cleared the high memory condition.

Explanation The Cisco Presence Engine service has cleared high memory condition and will now accept SIP messages

Recommended Action Notification purposes only; no action is required

Error Message

%UC_PE-6-PESipMessageTimeout: %[SipMessageCallID=String][AppID=String][ClusterID=String][NodeID=String]: Timeout occurred on SIP message transmission.

Explanation The transmission of an Cisco Presence Engine service SIP message timed out

Recommended Action Look for possible network latency problems

Error Message

%UC_PE-2-PESipSocketBindFailure: %[SipSocketInterface=String][AppID=String][ClusterID=String][NodeID=String]: Cisco Presence Engine service was unable to connect to the SIP listener interface.

Explanation Cisco Presence Engine service was unable to connect to the configured interface. No SIP traffic can be processed on this interface

Recommended Action Verify that the Cisco Presence Engine service listen interface is configured correctly on the IM and Presence Service Administration GUI Application Listener page. Verify that no other process is listening on the same port using netstat

Error Message

%UC_PE-6-PEStateStopped: %[AppID=String][ClusterID=String][NodeID=String]: Cisco Presence Engine service is terminating.

Explanation Cisco Presence Engine service is terminating

Recommended Action Notification purposes only; no action is required

Error Message

%UC_PE-4-PEStateLocked: %[AppID=String][ClusterID=String][NodeID=String]: Cisco Presence Engine service is administratively prohibited from processing traffic.

Explanation Cisco Presence Engine service is administratively prohibited from processing traffic

Recommended Action Notification purposes only; no action is required

Error Message

%UC_PE-6-PEStateShuttingdown: %[AppID=String][ClusterID=String][NodeID=String]: Cisco Presence Engine service is shutting down.

Explanation Cisco Presence Engine service is shutting down but will continue to process existing transactions. However, no new transactions will be processed

Recommended Action Notification purposes only; no action is required

Error Message

%UC_PE-6-PEStateUnlocked: %[AppID=String][ClusterID=String][NodeID=String]: Cisco Presence Engine service is administratively permitted to process traffic.

Explanation Cisco Presence Engine service is administratively permitted to process traffic

Recommended Action Notification purposes only; no action is required

Error Message

%UC_PE-4-PEStateDisabled: %[PEStateDisabledAlarmMessage=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco Presence Engine service is inoperable and unable to process traffic.

Explanation Cisco Presence Engine service is inoperable and unable to process traffic

Recommended Action Check the log files and monitor the Cisco Presence Engine service with RTMT

Error Message

%UC_PE-5-PEStateEnabled: %[PEStateEnabledAlarmMessage=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco Presence Engine service is now able to process traffic.

Explanation Cisco Presence Engine service is now able to process traffic

Recommended Action Notification purposes only; no action is required

Error Message

%UC_PE-3-PECalendarConnectionLoss: %[PECalendarConnectionLossAlarmMessage=String] [AppID=String][ClusterID=String][NodeID=String]: Indicates that the Cisco Presence Engine service cannot connect to the Calendar Server.

Explanation The Cisco Presence Engine service cannot connect to the Calendar Server and will fail all

calendar transactions until the connection is restored

Recommended Action Verify the Calendar Server is running and that the gateway configuration is correct on the IM and Presence Service Administration GUI Presence Gateways page

Error Message

%UC_PE-5-PECalendarConnectionLossCleared: %[PECalendarConnectionLossClearedAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: Cisco Presence Engine service has regained connection to the Calendar Server.

Explanation The Cisco Presence Engine service has successfully committed a transaction to the Calendar Server. The connection has been restored

Recommended Action Notification purposes only; no action is required

Error Message

%UC_PE-3-PEWebDAVInitializationFailure: %[PEWebDAVInitializationFailureAlarmMessage=String][AppID=String][ClusterID=String][NodeID=String]: Cisco Presence Engine service attempt to init the WebDAV library failed.

Explanation The Cisco Presence Engine service has failed to initialize the WebDAV library. The Calendaring feature will not work without WebDAV

Recommended Action Restart the Cisco Presence Engine service

Error Message

%UC_PE-3-PEWebDAVInitializationFailure: %[AppID=String][ClusterID=String][NodeID=String]: Cisco Presence Engine service attempt to init the WebDAV library failed.

Explanation The Cisco Presence Engine service has failed to initialize the WebDAV library. The Calendaring feature will not work without WebDAV

Recommended Action Restart the Cisco Presence Engine service

Error Message

%UC_Proxy-2-ESPStopped: %[Version=String][AppID=String][ClusterID=String][NodeID=String]: Cisco SIP Proxy service child process has been stopped.

Explanation Cisco SIP Proxy service child process has stopped

Recommended Action If the administrator has not manually stopped the Proxy service, this may indicate a problem. Please use RTMT to check for any related alarms

Error Message

%UC_Proxy-2-ESPSharedMemCreateFailed: %[AppID=String][ClusterID=String][NodeID=String]: Failed to create shared memory.

Explanation Failed to create shared memory segments while trying to initialize tables

Recommended Action Use RTMT to check system shared memory and check the Cisco SIP Proxy service trace log file for any detailed error messages

Error Message

%UC_Proxy-2-ESPSharedMemSetPermFailed: %[AppID=String][ClusterID=String] [NodeID=String]: Failed to set permissions on shared memory.

Explanation Failed to set permissions on shared memory segments while trying to initialize tables

Recommended Action Use RTMT to check system shared memory and check the Cisco SIP Proxy service trace log file for any detailed error messages

Error Message

%UC_Proxy-2-ESPSharedMemAllocFailed: %[MySQL=String][AppID=String][ClusterID=String] [NodeID=String]: Failed to allocate shared memory.

Explanation Failed to allocate shared memory segments while trying to initialize tables

Recommended Action Use RTMT to check system shared memory and check the Cisco SIP Proxy service trace log file for any detailed error messages

Error Message

%UC_Proxy-3-ESPConfigError: %[SharedMemorySize=String][NumberOfVsa=String][ENUM=String] [NumberExpansion=String][NumberServices=String][Registry=String][Routing=String][Radius=String] [RAS=String][RPMS=String][MethodRouting=String][AppID=String][ClusterID=String] [NodeID=String]: Cisco SIP Proxy service configuration file error.

Explanation This may indicate a formatting error, invalid value, etc with the Cisco SIP Proxy service configuration file

Recommended Action Verify that the Cisco Config Agent service is running. This service is responsible for writing the Proxy configuration file

Error Message

%UC_Proxy-3-ESPConfigNotFound: %[SipModule=String][SipAuthenModule=String][SipEnum=String] [SipNumExpand=String][SipNumServices=String][SipRegistry=String][SipRouting=String] [SipAcct=String][SipRpms=String][SipPrivacy=String][SipMethodRoute=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco SIP Proxy service configuration file not found.

Explanation This may indicate a formatting error, invalid value, etc, or even a missing configuration file

Recommended Action Verify that the configuration files /usr/local/sip/conf/sipd.conf and /usr/local/sip/conf/dynamic.sipd.conf exist on the IM and Presence server

Error Message

%UC_Proxy-3-ESPCreateLockFailed: %[AppID=String][ClusterID=String][NodeID=String]: Failed to create a lock file.

Explanation Failed to create a lock file

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

Error Message

%UC_Proxy-3-ESPSocketError: %[Radius=String][RAS=String][AppID=String][ClusterID=String] [NodeID=String]: Network socket errors encountered.

Explanation Network socket errors could be caused by binding errors, get socket address failures, etc

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

Error Message

%UC_Proxy-3-ESPStatsLogFileOpenFailed: %[AppID=String][ClusterID=String] [NodeID=String]: Failed to open stats log file.

Explanation Failed to open the Cisco SIP Proxy service stats log file

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

Error Message

%UC_Proxy-3-ESPStatsInitFailed: %[AppID=String][ClusterID=String][NodeID=String]: Failed to initialize the performance interface.

Explanation Failed to initialize the performance Interface

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

Error Message

%UC_Proxy-3-ESPMallocFailure: %[SIPProtocol=String][NumberExpansion=String][SipRegistry=String] [SipRouting=String][RAS=String][RPMS=String][AppID=String][ClusterID=String] [NodeID=String]: Failed to allocate memory.

Explanation Failed to allocate memory. This may indicate a low/no memory issue with the server

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

Error Message

%UC_Proxy-3-ESPWrongIPAddress: %[ProxyIPAddrTab=String][IPAddrNotMine=String] [DNSReturnedBadIP=String][ProxyLoopbackIPA=String][InvalidRASIPAddr=String] [InvalidRPMSIPAddr=String][AppID=String][ClusterID=String][NodeID=String]: Wrong IP address provided.

Explanation Wrong/invalid IP address was provided

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

Error Message

%UC_Proxy-3-ESPWrongHostName: %[AppID=String][ClusterID=String][NodeID=String]: Wrong host name.

Explanation This problem could be due to an invalid IP address, or an unresolvable hostname

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

Error Message

%UC_Proxy-3-ESPPassedParamInvalid: %[MySQL=String][ENUM=String][NumberExpansion=String] [RAS=String][AppID=String][ClusterID=String][NodeID=String]: Invalid parameter specified.

Explanation Invalid parameters were specified. This could be because the parameters were NULL

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

Error Message

%UC_Proxy-3-ESPNAPTRInvalidRecord: %[ENUM=String][AppID=String][ClusterID=String] [NodeID=String]: NAPTR record format error.

Explanation This error may indicate invalid flag fields, missing delimiter, etc

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

Error Message

%UC_Proxy-3-ESPVirtualProxyError: %[AppID=String][ClusterID=String] [NodeID=String]: Virtual_Proxy_Domain related error..

Explanation Virtual_Proxy_Domain related error.

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

Error Message

%UC_Proxy-3-ESPRegistryError: %[InvalidContact=String][ExceedMax=String] [RegistryDatabaseError=String][AppID=String][ClusterID=String][NodeID=String]: SIP Registry failure.

Explanation Unable to add registration to the SIP Registry because a resource limit was exceeded

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

Error Message

%UC_Proxy-3-ESPRoutingError: %[ExceedMax=String][RoutingDatabaseError=String][AppID=String] [ClusterID=String][NodeID=String]: SIP route interface error.

Explanation SIP Route Interface resource limit exceeded error

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

Error Message

%UC_Proxy-3-ESPLoginError: %[LoginDatabaseError=String][AppID=String][ClusterID=String] [NodeID=String]: Login datastore error.

Explanation Failed to connect or an error occurred while communicating with login datastore.

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

Error Message

%UC_Proxy-3-UASCBFindFailed: %[SCBFindFailure=String][AppID=String][ClusterID=String][NodeID=String]: SCB find failure.

Explanation A call to find_scb() returned NULL which indicates the SCB lookup failed

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

Error Message

%UC_Proxy-3-UASCBGetFailed: %[SCBGetFailure=String][AppID=String][ClusterID=String][NodeID=String]: SCB get or create failure.

Explanation A call to tcbtable_acquire_tcb() returned NULL which indicates a SCB get/create failure

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

Error Message

%UC_Proxy-6-CTIGWStarted: %[AppID=String][ClusterID=String][NodeID=String]: Cisco CTI Gateway application started.

Explanation Cisco CTI Gateway application started

Recommended Action Notification purposes only; no action is required

Error Message

%UC_Proxy-6-CTIGWStopped: %[AppID=String][ClusterID=String][NodeID=String]: Cisco CTI Gateway application stopped.

Explanation Cisco CTI Gateway application stopped

Recommended Action Notification purposes only; no action is required

Error Message

%UC_Proxy-4-CTIGWModuleNotEnabled: %[AppID=String][ClusterID=String][NodeID=String]: Cisco CTI Gateway application module is either not configured or enabled.

Explanation The Cisco CTI Gateway application is either not fully configured or enabled

Recommended Action Configure and enable the Cisco CTI Gateway application using the Cisco Unified CM IM and Presence CTI Gateway Settings page

Error Message

%UC_Proxy-6-CTIGWConnectionRestarted: %[AppID=String][ClusterID=String][NodeID=String]: CTI connection was restarted.

Explanation The CTI/QBE connection was restarted

Recommended Action Notification purposes only; no action is required

Error Message

%UC_Proxy-2-CTIGWProviderDown: %[AppID=String][ClusterID=String][NodeID=String]: CTI provider is down.

Explanation The CTI provider is currently unavailable

Recommended Action Check the connection to the configured Cisco Unified Callmanager nodes and verify the Cisco CTI Gateway application is enabled on the Cisco Unified CM IM and Presence Service CTI Settings page

Error Message

%UC_Proxy-4-CTIGWUserNotLicenced: %[AppID=String][ClusterID=String][NodeID=String]: User has no license.

Explanation User failed to authorize due to no license available

Recommended Action Check the Cisco CTI Gateway application license and user configuration

Error Message

%UC_Proxy-4-CTIGWUserNotAuthorized: %[AppID=String][ClusterID=String][NodeID=String]: User not authorized by CTI Gateway.

Explanation User failed to authorized due to wrong device or line DN

Recommended Action Verify user device configuration and MOC settings

Error Message

%UC_Proxy-2-CTIGWProviderFailedToOpen: %[AppID=String][ClusterID=String][NodeID=String]: CTI Provider failed to open.

Explanation CTI Provider failed to open due to a configuration error

Recommended Action Verify the Cisco Unified Callmanager address(es), and application user credentials on the Cisco Unified CM IM and Settings Service CTI Settings page

Error Message

%UC_Proxy-3-CTIGWQBEFailedRequest: %[AppID=String][ClusterID=String][NodeID=String]: QBE Request failure.

Explanation The Cisco CTI Gateway application received a failed response to a request

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

Error Message

%UC_Proxy-3-CTIGWSystemError: %[CSTAError=String][InternalError=String][GeneralError=String][AppID=String][ClusterID=String][NodeID=String]: Cisco CTI Gateway application system errors.

Explanation Cisco CTI Gateway application system errors

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

Error Message

%UC_Proxy-3-PWSSCBFindFailed: %[SCBFindFailure=String][AppID=String][ClusterID=String][NodeID=String]: SCB find failure.

Explanation A call to find_scb() returned NULL which indicates the SCB lookup failed

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

Error Message

%UC_Proxy-3-PWSSCBInitFailed: %[SCBInitFailure=String][AppID=String][ClusterID=String][NodeID=String]: SCB init failure.

Explanation SCB init failed

Recommended Action Restart the Cisco SIP Proxy service

Error Message

%UC_Proxy-5-PWSBelowCPULimit: %[BelowCPULimit=String][AppID=String][ClusterID=String][NodeID=String]: CPU utilization has fallen below the max CPU limit.

Explanation CPU utilization has fallen below the max CPU limit, new requests will no longer be blocked

Recommended Action Notification purposes only; no action is required

Error Message

%UC_Proxy-4-PWSAboveCPULimit: %[AboveCPULimit=String][AppID=String][ClusterID=String][NodeID=String]: Indicates the Presence Web Service has exceeded a CPU utilization threshold.

Explanation The Presence Web Service module running in the Cisco SIP Proxy service has detected that the CPU utilization has exceeded the configured threshold. During this time new requests will be blocked until the CPU utilization drops below the configured threshold

Recommended Action Using RTMT, inspect the Cisco SIP Proxy service logs for more details

Error Message

%UC_Proxy-4-PWSRequestLimitReached: %[RequestLimitReached=String][AppID=String][ClusterID=String][NodeID=String]: Proxy service request per second limit reached.

Explanation The Cisco SIP Proxy service request per second limit has been reached

Recommended Action You may need to throttle back the incoming request rate

Error Message

%UC_Proxy-4-PWSAboveSipSubscriptionLimit: %[AboveSipSubscriptionLimit=String][AppID=String][ClusterID=String][NodeID=String]: Indicates the Presence Web Service subscription count has exceeded the maximum limit.

Explanation The Presence Web Service running in the Cisco SIP Proxy service has detected that the subscription count has exceeded the configured limit. During this time the Presence Web Service will block new incoming SIP subscriptions until the subscription count drops below the configured limit

Recommended Action Using RTMT, inspect the Cisco SIP Proxy service logs for more details

Error Message

%UC_Proxy-5-PWSBelowSipSubscriptionLimit: %[BelowSipSubscriptionLimit=String][AppID=String][ClusterID=String][NodeID=String]: Subscriptions have fallen below the max limit.

Explanation The Presence Web Service running in the Cisco SIP Proxy service has detected that the subscription count has fallen below the configured limit

Recommended Action Notification purposes only; no action is required

Error Message

%UC_SoapAPI-4-LegacyCUPCLogin: %[userid=String][version=String][AppID=String]

[ClusterID=String][NodeID=String]: A legacy Cisco Unified Personal Communicator client attempted to login to the Cisco Client Profile Agent service.

Explanation A legacy Cisco Unified Personal Communicator client attempted to login to the Cisco Client Profile Agent service. Login was denied

Recommended Action Please upgrade the legacy Cisco Unified Personal Communicator client as it is currently not supported

Error Message

%UC_SA-2-SyncAgentAXLConnectionFailed: %[AppID=String][ClusterID=String] [NodeID=String]: Cisco Sync Agent service failed authentication.

Explanation Cisco Sync Agent service failed authentication to the remote Cisco Unified Communications Manager publisher and therefore is unable to connect

Recommended Action Please verify the AXL credentials are correct and whether the Cisco AXL Web service is activated and running on the remote Cisco Unified Communications Manager publisher

Error Message

%UC_SA-2-NotInCucmServerListError: %[AppID=String][ClusterID=String][NodeID=String]: Cisco Sync Agent failed to start up because the IM and Presence node is not in the server list, or has been deleted and then readded to the server list on the Cisco Unified Communications Manager publisher..

Explanation The IM and Presence Server node is not in the server list, or has been deleted and then readded to the server list on the Cisco Unified Communications Manager publisher.

Recommended Action Please add the IM and Presence node in the server list on the Cisco Unified Communications Manager server and reinstall the IM and Presence node.

Error Message

%UC_SRM-2-SRMFailover: %[FromNode=String][ToNode=String][Reason=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco SRM is performing an automatic failover.

Explanation Cisco SRM is performing an automatic failover

Recommended Action Please verify that the failed node is up and that critical services are running.

Error Message

%UC_SRM-2-SRMFailed: %[AppID=String][ClusterID=String][NodeID=String]: Cisco Server Recovery Manager is in the failed state.

Explanation Cisco SRM is in the failed state

Recommended Action Please restart the Cisco Server Recovery Manager.

Error Message

%UC_Xcp-3-XcpDBConnectError: %[AppID=String][ClusterID=String][NodeID=String]: Cisco XCP data acces layer was unable to connect to the DB..

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

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

Error Message

%UC_Xcp-6-XcpDBConnectRestore: %[AppID=String][ClusterID=String][NodeID=String]: Cisco XCP data access layer was able to restore connection to the DB..

Explanation Cisco XCP data access layer was able to restore connection to the DB. The alert condition, if any, caused by the connection failure will be cleared.

Recommended Action None.

Error Message

%UC_Xcp-3-XcpComponentConnectError: %[AppID=String][ClusterID=String][NodeID=String]: The XCP component failed to connect to the XCP Router. The component is shutting down. .

Explanation The concerned XCP component failed to connect to the XCP Router. The component is shutting down after reaching the configured number of reconnect attempts.

Recommended Action Please check the component log file for more details.

Error Message

%UC_Xcp-3-XcpComponentConfigError: %[AppID=String][ClusterID=String][NodeID=String]: The XCP component detected a bad configuration. .

Explanation The concerned XCP component failed to load the configuration due to an error. This may be due to an invalid element in the configuration file.

Recommended Action Please check the component log file for more details.

Error Message

%UC_Xcp-3-XcpMdnsStartError: %[AppID=String][ClusterID=String][NodeID=String]: The XCP Router failed to startup the MDNS. .

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

Recommended Action Please check the XCP Router log file for more details.

Error Message

%UC_Xcp-3-XcpCmPauseSockets: %[AppID=String][ClusterID=String][NodeID=String]: The XCP Router has directed the XCP Connection Manager (CM) to pause listening on its socket due to load on the system..

Explanation Outstanding XCP internal packet or database requests have reached configured limit. Client connections will be paused until pending requests have dropped back below threshold. Users will experience lag until issue is resolved. Users may be disconnected if configured timeout is reached before resolution.

Recommended Action Please check the XCP Router log file for more details. Watch for client disconnecting due to timeout from the XCP Connection Managers.

Error Message

%UC_Xcp-6-XcpCmResumeSockets: %[AppID=String][ClusterID=String][NodeID=String]: Outstanding internal packet or database requests have dropped back below configured threshold..

Explanation XCP Connection Manager has been notified to resume listening on client connections.

Recommended Action Please check the XCP Router log file for more details.

Error Message

%UC_Xcp-3-XcpCmStartupError: %[AppID=String][ClusterID=String][NodeID=String]: The XCP Connection Manager service failed to startup. .

Explanation The XCP Connection Manager (CM) service failed to startup. One of the configured CM Directors may have failed to startup.

Recommended Action Please check the CM log file for more details.

Error Message

%UC_Xcp-3-XcpCmHttpdError: %[AppID=String][ClusterID=String][NodeID=String]: The XCP Connection Manager service has errors in the HTTP interface. .

Explanation The XCP Connection Manager (CM) service has errors in the HTTP interface. This can cause connectivity failures to HTTP based clients.

Recommended Action Please check the CM log file for more details.

Error Message

%UC_Xcp-3-XcpCmXmppdError: %[AppID=String][ClusterID=String][NodeID=String]: The XCP Connection Manager service has errors in the XMPP interface. .

Explanation The XCP Connection Manager (CM) service has errors in the XMPP interface. This can cause connectivity failures to XMPP based clients.

Recommended Action Please check the CM log file for more details.

Error Message

%UC_Xcp-3-XcpTxtConfGearError: %[AppID=String][ClusterID=String][NodeID=String]: The XCP Text Conference Manager Service failed to load a configured gear. .

Explanation The XCP Text Conference Manager (TC) Service has failed to load a configured component. This can prevent the service to start or behave as expected.

Recommended Action Please check the XCP Text Conference log file for more details.

Error Message

%UC_Xcp-6-XcpTxtConfRoomLimitError: %[AppID=String][ClusterID=String][NodeID=String]: This server has a limit on the maximum number of supported text conference rooms. .

Explanation There is a maximum limit of 16500 text conference rooms per server. This limit is the combined total of both persistent chat rooms and adhoc chat rooms.

Recommended Action In order to increase the maximum supported text chat room capacity, additional servers must be deployed.

Error Message

%UC_Xcp-3-XcpTxtConfDbQueueSizeLimitError: %[AppID=String][ClusterID=String] [NodeID=String]: The number of DB requests has reached the maximum limit specified by the configuration..

Explanation The TC service queues database requests to the external database. If the database server is overloaded or is not accessible, database requests will be queued by the TC service. Once the queue size exceeds the configurable threshold, database requests will be discarded. This may result in persistent room data or messages not being saved to the database.

Recommended Action Check the state of the external database server and check that it is accessible over the network. Then restart the Cisco XCP Text Conference Manager on CUP.

Error Message

%UC_Xcp-3-XcpTxtConfTCMessagesMsgIdError: %[AppID=String][ClusterID=String] [NodeID=String]: Invalid state of table tc_messages in the external database used for persistent chat.

Explanation The value of msg_id in tc_messages table is higher than the value used for generating new msg_ids from xcp_sequence table.

Recommended Action On the external database used for persistent chat, update the value of xcp_sequence.new_id where the name_id is 'tc_message_id' to the next value higher than max(msg_id) from tc_messages that is also a multiple of 100, plus 1. Then restart the Cisco XCP Text Conference Manager on IM and Presence Server.

Error Message

%UC_Xcp-2-XcpSIPGWStackResourceError: %[AppID=String][ClusterID=String][NodeID=String]: The number of concurrent S2S SIP Federation subscriptions or call-legs has reached the maximum limit specified by the configuration..

Explanation The number of concurrent S2S SIP Federation subscriptions or call-legs has reached the maximum limit specified by the configuration. It will not be possible to create any more subscriptions or call-legs at the time.

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

Error Message

%UC_Xcp-3-XcpThirdPartyComplianceConnectError: %[complianceserver=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco XCP Router is unable to connect to Third Party Compliance Server.

Explanation Cisco XCP Router is unable to connect to Third Party Compliance Server. This may be because of a network problem or a Third Party Compliance Server config or licensing problem

Recommended Action This is a serious error that breaks IM on the IM and Presence Service. Check network connection to and configuration(including licensing) on Third Party Compliance Server. To restore IM services set the Compliance Settings option in the Admin GUI to "Not Configured" until the connection failure cause has been identified

Error Message

%UC_Xcp-6-XcpThirdPartyComplianceConnectRestore: %[complianceserver=String][AppID=String][ClusterID=String][NodeID=String]: Cisco XCP Router is reconnected to Third Party Compliance Server.

Explanation Cisco XCP Router is reconnected to Third Party Compliance Server. This indicates an initial connection or reconnection

Recommended Action None.

Error Message

%UC_Xcp-3-XcpMFTExtFsMountErrorStart: %[AppID=String][ClusterID=String][NodeID=String]: Cisco XCP File Transfer Manager has lost its connection to the external file server.

Explanation Cisco XCP File Transfer Manager has lost its connection to the external file server.

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

Error Message

%UC_Xcp-5-XcpMFTExtFsMountErrorEnd: %[AppID=String][ClusterID=String][NodeID=String]: Cisco XCP File Transfer Manager was able to re-establish its connection to the external file server.

Explanation Cisco XCP File Transfer Manager was able to re-establish its connection to the external file server.

Recommended Action This alarm is for information purposes only; no action is required.

Error Message

%UC_Xcp-3-XcpMFTExtFsFreeSpaceWarnStart: %[AppID=String][ClusterID=String][NodeID=String]: Cisco XCP File Transfer Manager has detected that the available disk space on the external file server is low.

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

Recommended Action Please free up space on the external file server by deleting unwanted files from the partition used for file transfer.

Error Message

%UC_Xcp-5-XcpMFTExtFsFreeSpaceWarnEnd: %[AppID=String][ClusterID=String] [NodeID=String]: CCisco XCP File Transfer Manager has detected that there is sufficient disk space on the external file server.

Explanation Cisco XCP File Transfer Manager has detected that there is sufficient disk space on the external file server.

Recommended Action This alarm is for information purposes only; no action is required.

Error Message

%UC_Xcp-3-XcpComponentWriteAlarmYellow: %[component=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco XCP Router - Component's MIO Write buffer's nominal capacity exceeded

Explanation Component's MIO Write buffer's exceeded 50K write buffer

Recommended Action None

Error Message

%UC_Xcp-3-XcpComponentWriteAlarmOrange: %[component=String][AppID=String] [ClusterID=String][NodeID=String]: Cisco XCP Router - Component's MIO Write buffer's warning capacity exceeded

Explanation Component's MIO Write buffer's exceeded 80K write buffer

Recommended Action None

Error Message

%UC_Xcp-3-XcpComponentWriteAlarmRed: %[component=String][AppID=String][ClusterID=String] [NodeID=String]: Cisco XCP Router - Component's MIO Write buffer's critical capacity exceeded

Explanation Component's MIO Write buffer's exceeded 100K write buffer

Recommended Action None

Error Message

%UC_XcpCM-2-XCPConfigMgrJabberRestartRequired: %[AppID=String][ClusterID=String] [NodeID=String]: Cisco XCP Config Manager has regenerated XCP XML files after system halt due to buffer size. The XCP Router must now be restarted to pick up changes..

Explanation Cisco XCP Config Manager has regenerated XCP XML files after system halt due to buffer size. The XCP Router must now be restarted to pick up changes .

Recommended Action Restart the XCP Router.

Error Message

%UC_XcpCM-2-XCPConfigMgrConfigurationFailure: %[realm=String][component=String] [AppID=String][ClusterID=String][NodeID=String]: Cisco XCP Config Manager was unable to send configuration to a component. Please check logs..

Explanation Cisco XCP Config Manager failed to successfully update XCP Configuration.

Recommended Action See Cisco XCP Config Manager logs for further root cause.

Error Message

%UC_XcpCM-2-XCPConfigMgrHostNameResolutionFailed: %[hostname=String][AppID=String]

[ClusterID=String][NodeID=String]: XCP Config manager hostname resolution failed.

Explanation Cisco XCP Config Manager could not resolve a DNS name to allow XCP Routers to connect to that node.

Recommended Action Please verify DNS resolvability of all Hostnames and FQDNs in both local and remote clusters. Restart XCP Config Manager then XCP Router after DNS is resolvable.

Error Message

%UC_XcpCM-2-XCPConfigMgrR2RPasswordEncryptionFailed: %[hostname=String][AppID=String] [ClusterID=String][NodeID=String]: XCP Config Manager Password Encryption Failed.

Explanation Cisco XCP Config Manager was unable to encrypt the password associated with an Inter-cluster Router-to-Router configuration.

Recommended Action Restart XCP Config Manager and then restart the XCP Router

Error Message

%UC_XcpCM-2-XCPConfigMgrR2RRequestTimedOut: %[hostname=String][AppID=String] [ClusterID=String][NodeID=String]: XCP Config Manager R2R Configuration Request Timed Out.

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

Recommended Action Restart XCP Config Manager and then restart the XCP Router

Error Message

%UC_XcpCM-2-XCPExternalDatabaseCertificateNotFound: %[AppID=String][ClusterID=String] [NodeID=String]: Cisco XCP Config Manager was unable to find one or more external Database certificates from cup-xmpp-trust store

Explanation An attempt to establish an SSL connection between the Cisco Unified IM and Presence Service node and the configured External Database has failed because the required certificate is missing.This may have occurred as a result of the Cisco Inter Cluster Sync Agent (ICSA) service not having propagated the certificate to all nodes yet or the required certificate has been deleted.

Recommended Action Please ensure that the required certificate is uploaded to the cup-xmpp-trust store. If the certificate is already present, please ensure that the Cisco ICSA service is running on all the IM and Presence service nodes. Restart the Cisco ICSA service on all the nodes or wait for 15 minutes to ensure that the Cisco ICSA service propagates the certificate to all the IM and Presence service nodes. As an additional step, please navigate to the External Database configuration page for the particular database and take corrective measures if there are any error messages displayed on the page. Finally, restart the Cisco XCP Config Manager Service.

Error Message

%UC_XcpCM-2-PushNotificationFailed: %[Type=String][TrackingID=String][SourceUserJID=String] [DestinationUserJID=String][ErrorCode=String][ErrorDescription=String][component=String] [AppID=String][ClusterID=String][NodeID=String]: Cisco XCP Config Manager was not able to send Push Notification.

Explanation An attempt to send a message packet to PushUri failed, Push Notification not sent

Recommended Action Take action as appropriate based on the Error Code and Error Description. If further assistance is required, please contact Cisco Technical Support.

Error Message

%UC_XcpCM-2-PushNotificationFailedInvalidDeviceToken: %[Type=String][TrackingID=String] [SourceUserJID=String][DestinationUserJID=String][ErrorCode=String][ErrorDescription=String] [component=String][AppID=String][ClusterID=String][NodeID=String]: Cisco XCP Config Manager was not able to send Push Notification.

Explanation An attempt to send a Push Notification to Cisco Cloud(Push Microservice) failed due to an invalid device token.

Recommended Action Have the impacted user attempt to logout and log back in to Jabber. If this does not resolve the issue, please contact Cisco Technical Support.

Error Message

%UC_XcpCM-2-PushNotificationFailedInvalidAccessToken: %[Type=String][TrackingID=String] [SourceUserJID=String][DestinationUserJID=String][ErrorCode=String][ErrorDescription=String] [component=String][AppID=String][ClusterID=String][NodeID=String]: Cisco XCP Config Manager was not able to send Push Notification.

Explanation An attempt to send a Push Notification to Cisco Cloud(Push Microservice) failed due to an invalid access token.

Recommended Action Inspect the IMnPresence XCP Config Manager service logs to ensure the AccessToken was fetched and refreshed in a timely manner. If this was done in a timely manner, then the issue may be on the Cisco Cloud side. In that case, please contact Cisco Technical Support for further debugging.

Error Message

%UC_XcpCM-2-AccessTokenFetchFailed: %[Type=String][ErrorCode=String][ErrorDescription=String] [component=String][AppID=String][ClusterID=String][NodeID=String]: Cisco XCP Config Manager was unable to fetch the Access Token

Explanation Cisco XCP Config Manager was unable to fetch the access token

Recommended Action Take action as appropriate based on the Error Code and Error Description. If further assistance is required, please contact Cisco Technical Support.

Error Message

%UC_XcpCM-2-InvalidPushPacket: %[Type=String][ErrorDescription=String][component=String] [AppID=String][ClusterID=String][NodeID=String]: Cisco XCP Config Manager was not able to send Push Notification.

Explanation An attempt to send a Push Notification to Cisco Cloud(Push Microservice) failed due to an Invalid Push Packet.

Recommended Action Take action as appropriate based on the Error Description. Further analysis may require investigation including the Client and server-side XCP Router service. If further assistance is required, please contact Cisco Technical Support.

Error Message

%UC_XcpCM-2-PushXMPPClientPoolError: %[Type=String][ErrorDescription=String] [component=String][AppID=String][ClusterID=String][NodeID=String]: Cisco XCP Config Manager was not able to send Push Notification.

Explanation Encountered an issue while establishing HTTP client pool connection from Config Manager to Cisco Cloud.

Recommended Action [Note: the following recovery techniques will impact multiple clients; please plan accordingly as to when these activities are performed] Within the Unified CM configuration, set Push to 'Disable', then back to 'Enable.' If this is unsuccessful, restart the Cisco XCP Config Manager service. For further assistance please contact Cisco Technical Support.

Error Message

%UC_XcpCA-3-XCAPollingThreadExited: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: Cisco XCP Counter Aggregator service has its polling thread exited..

Explanation Cisco XCP Counter Aggregator service has its polling thread exited.

Recommended Action Check log file for any errors. Try restarting the Cisco XCP Counter Aggregator service.

Error Message

%UC_SAMLSSO-6-SAMLSSOEnableSuccess: %[AppID=String][ClusterID=String] [NodeID=String]: SAML SSO enable operation successful.

Explanation This alarm indicates that operation to enable SAML SSO was successful.

Recommended Action Informational alarm. No action required.

Error Message

%UC_SAMLSSO-3-SAMLSSOEnableFailure: %[ErrorDetails=String][AppID=String][ClusterID=String] [NodeID=String]: SAML SSO enable operation failed.

Explanation This alarm indicates that operation to enable SAML SSO has failed.

Recommended Action In the Cisco Unified Reporting tool, run a CM Cluster Overview report and check the SAML SSO status on other nodes in the cluster to determine if operation has failed on other nodes as well. Verify that there is connectivity between the node from where the enable operation is initiated and the node(s) where the operation failed. Use RTMT to collect traces for Cisco SSO and contact Cisco TAC for assistance. Alternately, use CLI to collect traces by running the commands 'file get activelog tomcat/logs/ssosp/log4j/*.log' and 'file get activelog platform/log/ssoApp*.log'.

Error Message

%UC_SAMLSSO-6-SAMLSSODisableSuccess: %[AppID=String][ClusterID=String] [NodeID=String]: SAML SSO disable operation successful.

Explanation This alarm indicates that operation to disable SAML SSO was successful.

Recommended Action Informational alarm. No action required.

Error Message

%UC_SAMLSSO-3-SAMLSSODisableFailure: %[ErrorDetails=String][AppID=String][ClusterID=String] [NodeID=String]: SAML SSO disable operation failed.

Explanation This alarm indicates that operation to disable SAML SSO has failed.

Recommended Action In the Cisco Unified Reporting tool, run a CM Cluster Overview report and check the SAML SSO status on other nodes in the cluster to determine if operation has failed on other nodes as well. Verify that there is no connectivity issues between the node from where the disable operation is initiated and the node(s) where the operation failed. If the disable operation was performed from the web pages, the same can be tried from the CLI (of the node where the disable failed) using command "utils sso disable". If the disable still fails, use RTMT to collect traces for Cisco SSO and contact Cisco TAC for assistance. Alternately, use CLI to collect traces by running the commands 'file get activelog tomcat/logs/ssosp/log4j/*.log' and 'file get activelog platform/log/ssoApp*.log'.

Error Message

%UC_LPMTCT-4-LogPartitionLowWaterMarkExceeded: %[UsedDiskSpace=String] [{Optional}MessageString=String][AppID=String][ClusterID=String][NodeID=String]: The percentage of used disk space in the log partition has exceeded the configured low water mark..

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

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.

Error Message

%UC_LPMTCT-2-LogPartitionHighWaterMarkExceeded: %[UsedDiskSpace=String] [{Optional}MessageString=String][AppID=String][ClusterID=String][NodeID=String]: The percentage of used disk space in the log partition has exceeded the configured high water mark..

Explanation 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.

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.

Error Message

%UC_LPMTCT-6-LogFileSearchStringFound: %[SearchString=String][AppID=String][ClusterID=String][NodeID=String]: The search string has been found in the log file..

Explanation Trace and Log Central has found the search string that the user has configured

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.

Error Message

%UC_LPMTCT-4-LogCollectionJobLimitExceeded: %[JobType=String][AppID=String][ClusterID=String][NodeID=String]: The number of Log Collection Jobs have excceded the allowed limit.

Explanation 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.

Recommended Action Cancel one or more of the currently running queries and try again to configure the trace collection.

Error Message

%UC_LPMTCT-3-ScheduledCollectionError: %[JobID=String][Reason=String][AppID=String][ClusterID=String][NodeID=String]: An error occurred while executing scheduled collection..

Explanation Scheduled collection encountered an error during execution.

Recommended Action Review configuration for scheduled collection job under Job Status window.

Error Message

%UC_LPMTCT-2-CoreDumpFileFound: %[TotalCoresFound=String][CoreDetails=String][Core1=String][Core2=String][Core3=String][Core4=String][Core5=String][Core6=String][AppID=String][ClusterID=String][NodeID=String]: The new core dump file(s) have been found in the system..

Explanation One of the component has crashed and generated a core dump. Use admin cli or RTMT to featch the backtrace.

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.

Error Message

%UC_LPMTCT-3-SparePartitionLowWaterMarkExceeded: %[UsedDiskSpace=String][{Optional}MessageString=String][AppID=String][ClusterID=String][NodeID=String]: The percentage of used disk space in the spare partition has exceeded the configured low water mark..

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

Recommended Action Login into RTMT and check the configured threshold value for SparePartitionLowWaterMarkExceeded 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.

Error Message

%UC_LPMTCT-4-SparePartitionHighWaterMarkExceeded: %[UsedDiskSpace=String] [{Optional}MessageString=String][AppID=String][ClusterID=String][NodeID=String]: The percentage of used disk space in the spare partition has exceeded the configured high water mark..

Explanation 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

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.

Error Message

%UC_LPMTCT-4-AuditLogOverflowDueToLPMPurge: %[AppID=String][ClusterID=String] [NodeID=String]: Indicates that application audit log files have been deleted by Log Partition Monitor(LPM).

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

Recommended Action Login to " Cisco Unified Serviceability - > Tools - > Audit Log Configuration " page and check if the purging is enabled. You can choose not to delete the audit log files by LPM by disabling the " Enable Purging " option.

Error Message

%UC_CALLMANAGER-2-CallManagerFailure: %[{Optional}Text=String][HostName=String] [IPAddress=String][Reason=Enum][AppID=String][ClusterID=String][NodeID=String]: Indicates an internal failure in Unified CM.

Explanation This alarm indicates that an internal failure occurred in the Cisco CallManager service. The service should restart in an attempt to clear the failure.

Recommended Action Monitor for other alarms and restart Cisco CallManager service, if necessary. Collect the core file if available, SDL and CCM/SDI trace files (you can gather these from Trace and Log Central in RTMT using the Collect Files feature) and contact the Cisco Technical Assistance Center (TAC).

Reason Code - Enum Definitions

Enum Definitions - Reason

Value	Definition

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

Error Message

%UC_CALLMANAGER-5-SDLLinkISV: %[RemoteIPAddress=String][LinkID=String][LocalNodeId=UInt][LocalApplicationId=Enum][RemoteNodeID=UInt][RemoteApplicationId=Enum][AppID=String][ClusterID=String][NodeID=String]: SDL link to remote application restored.

Explanation This alarm indicates that the local Unified CM has gained communication with the remote Unified CM. Note that the remote Unified CM should also indicate SDLLinkISV with a different LinkID.

Recommended Action Informational only; no action is required

Reason Code – Enum Definitions

Enum Definitions – LocalApplicationId

Value	Definition
100	CallManager

Enum Definitions – RemoteApplicationId

Value	Definition
100	CallManager

Error Message

%UC_CALLMANAGER-1-SDLLinkOOS: %[RemoteIPAddress=String][LinkID=String][LocalNodeId=UInt][LocalApplicationID=Enum][RemoteNodeID=UInt][RemoteApplicationID=Enum][AppID=String][ClusterID=String][NodeID=String]: SDL link to remote application is out of service.

Explanation 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).

Recommended Action In the Cisco Unified Reporting tool, run a CM Cluster Overview report and check to see if all servers can communicate with 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.

Reason Code - Enum Definitions

Enum Definitions - LocalApplicationID

Value	Definition
100	CallManager

Enum Definitions - RemoteApplicationID

Value	Definition
100	CallManager

Error Message

%UC_CALLMANAGER-1-CMVersionMismatch: %[RemoteAppProtocolVersion=String] [LocalAppProtocolVersion=String][RemoteNodeId=UInt][RemoteAppId=Enum] [RemoteAppVersion=String][AppID=String][ClusterID=String][NodeID=String]: One or more Unified CM nodes in a cluster are running different Unified CM versions.

Explanation 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.

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.

Reason Code - Enum Definitions

Enum Definitions - RemoteAppId

Value	Definition
100	CallManager
200	CTIManager
300	CMI

Error Message

%UC_CALLMANAGER-2-BChannelOOS: %[ChannelKey=String][DeviceName=String][Reason=Enum] [ChannelId=UInt][AppID=String][ClusterID=String][NodeID=String]: The B-channel is out of service.

Explanation 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: Taking the channel out of service intentionally to perform maintenance on either the near-end or far-end; Losing T1/E1/BRI cable connectivity; When the MGCP gateway returns an error code 501 or 510 for a MGCP command sent from Unified CM; When the MGCP gateway doesn't respond to an MGCP command sent by Unified CM three times; When a speed and duplex mismatch exists on the Ethernet port between Unified CM and the MGCP gateway.

Recommended Action Check the Cisco CallManager 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; Check the connection of the T1/E1/BRI cable; Reset the MGCP gateway;

Check the speed and duplex settings on the Ethernet port.

Reason Code - Enum Definitions

Enum Definitions - Reason

Value	Definition
0	None Defined

Error Message

%UC_CALLMANAGER-5-BChannelISV: %[ChannelId=UInt][ChannelKey=String][DeviceName=String] [AppID=String][ClusterID=String][NodeID=String]: B-channel is in service.

Explanation The B-channel indicated by this alarm has gone in service

Recommended Action Informational purposes only; no action is required

Error Message

%UC_CALLMANAGER-2-DChannelOOS: %[ChannelId=UInt][ChannelKey=String][DeviceName=String] [IPAddress=String][Reason=Enum][AppID=String][ClusterID=String][NodeID=String]: The D-channel is out of service.

Explanation The D-channel indicated by this alarm has gone out of service. Common reasons for a D-channel to go 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 a gateway reset.

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.

Reason Code - Enum Definitions

Enum Definitions - Reason

Value	Definition
0	None Defined

Error Message

%UC_CALLMANAGER-5-DChannelISV: %[ChannelId=UInt][ChannelKey=String][DeviceName=String] [IPAddress=String][AppID=String][ClusterID=String][NodeID=String]: D-channel is in service.

Explanation The indicated D-channel has gone in service

Recommended Action Notification purposes only; no action is required

Error Message

%UC_CALLMANAGER-4-DeviceTransientConnection: %[{Optional}IPAddress=String] [{Optional}DeviceName=String][{Optional}MACAddress=String][Protocol=String] [{Optional}DeviceType=Enum][{Optional}Reason=Enum][ConnectingPort=UInt] [{Optional}SIPUser=String][{Optional}IPV6Address=String][{Optional}IPAddrAttributes=Enum] [{Optional}IPV6AddrAttributes=Enum][AppID=String][ClusterID=String][NodeID=String]: A device attempted to register but did not complete registration.

Explanation 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.

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 in the alarm for recommended actions. No action is required if this event was issued as a result of a normal device rehome.

Reason Code - Enum Definitions

Enum Definitions - DeviceType

Value	Definition
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
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
254	UNKNOWN_MGCP_GATEWAY
255	UNKNOWN
30027	ANALOG_PHONE
30028	ISDN_BRI_PHONE
30032	SCCP_GATEWAY_VIRTUAL_PHONE

Enum Definitions - Reason

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 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.
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 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.
6	ConnectivityError - The network connection between the device and 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 Unified CM node is experiencing high CPU usage. Verify that the device is powered up and operating, verify that there is network connectivity between the device and Unified CM, and verify the CPU utilization is in the safe range (you can monitor this via the CPU Pegging Alert in RTMT).
7	InitializationError – An internal error occurred within Unified CM while processing the device registration. Cisco recommends that you restart the Cisco CallManager service. If this issue 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 the Cisco Technical Assistance Center (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 that the information in the Digest Credentials field on the End User Configuration page is configured. Also, check the Phone Configuration page to determine whether 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 that the digest credentials configured on the phone match the Digest Credentials configured in the End User Configuration page.
11	InvalidX509NameInCertificate – Configured "X.509 Subject Name" doesn't match the information in the certificate from the device. Check the Security profile of the indicated device and verify that the Device Security Mode is set to either Authenticated or Encrypted. Verify that the X.509 Subject Name field has the appropriate content; it should match the Subject Name in the certificate from the peer.
12	InvalidTLSCipher – Unsupported cipher algorithm used by the device; 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, or an expires value that is too small. Check the REGISTER message for any of these issues and if you find one, correct the issue.
15	ProtocolMismatch - The protocol of the device (SIP or SCCP) does not match the configured protocol in Unified CM. Recommended actions: 1) Verify that the device is configured with the appropriate protocol; 2) Verify that the firmware load ID on the Device Defaults page in Cisco Unified CM Administration is correct and actually exists on the TFTP server; 3) If there is a firmware load ID configured on the Device Configuration page, verify that it is correct and that it exists on the TFTP server (on Cisco Unified OS Administration page, access Software Upgrades > TFTP File Management, then 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 that 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 the Cisco Technical Assistance Center (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 Configuration page, verify that the firmware load ID exists on the TFTP server (on Cisco Unified OS Administration page, access Software Upgrades > TFTP File Management, then look for the file name as specified by load ID).
23	DatabaseTimeout – 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 Unified CM at an unexpected time and Unified CM had not yet obtained the requested information. The device will automatically attempt to register again. If this alarm occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be an internal firmware error. Collect existing SDI and SDL traces and contact the Cisco Technical Assistance Center (TAC).
26	InvalidCapabilities – (SCCP only) Unified CM detected an error in the media capabilities reported in the StationCapabilitiesRes message by the device during registration. The device will automatically attempt to register again. If this alarm occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be a protocol error. Collect existing SDI and SDL traces and contact the Cisco Technical Assistance Center (TAC).
27	CapabilityResponseTimeout – (SCCP only) Unified CM timed out while waiting for the device to respond to a request to report its media capabilities. 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 that the device is powered up and operating, verify that network connectivity exists between the device and Unified CM, and verify that the CPU utilization is in the safe range (you can monitor this via the CPU Pegging Alert in RTMT).

28	SecurityMismatch - Unified CM detected a mismatch in the security settings of the device and/or Unified CM. This alarm can occur due to any of the following situations: The device established a secure connection yet reported that it does not have the ability to do authenticated signaling; the device did not establish a secure connection but the security mode configured for the device indicates that it should have done so; or the device established a secure connection but the security mode configured for the device indicates that it should not have done so. To correct the error, ensure that the security settings of the device and Unified CM are correct for your deployment. Resetting the device may help because it forces the device to download its latest settings. If the device is a Cisco phone, verify that the TFTP service is running and reachable by the phone and view the Unified CM Database Status report in Cisco Unified Reporting to verify that database replication is Good. You can also issue the following command on the CLI to view database replication: utils dbreplication runtimestate.
29	AutoRegisterDBError - Auto-registration of a device failed because auto-registration is not allowed for the device type or because an error occurred while adding the auto-registering device to the database (stored procedure). Note that if Unified CM is in mixed mode (System > Enterprise Parameters > Cluster Security Mode = 1), auto-registration is not allowed and the device must be configured manually. If you are not planning to auto-register phones, either manually configure the phone (Device > Phone > Add New), power the device down, or remove it from the network. If you are attempting to auto-register this phone, verify that the cluster is not in mixed mode (System > Enterprise Parameters > Cluster Security Mode = 1) and verify that auto-registration is enabled on the node to which this device is registering (System > Cisco Unified CM > ensure that the Auto-registration Disabled... checkbox is not checked).
30	DBAccessError - Device registration failed because of an error that occurred while building

	the station registration profile. This usually indicates a synchronization problem with the database. View the Unified CM Database Status report in Cisco Unified Reporting to verify that database replication is Good. You can also issue the following command on the CLI to view database replication: utils dbreplication runtimestate. When database replication is Good on all nodes, restart the Cisco CallManager service on the node to which the device is attempting to register. If the problem persists, collect SDI and SDL traces for the Cisco Database layer Monitor service and contact the Cisco Technical Assistance Center (TAC).
31	AutoRegisterDBConfigTimeout - (SCCP only) 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. The device will automatically attempt to register again. Check for high CPU utilization on this Unified CM node because congestion could be a cause of this alarm. If this alarm continues to occur, restart the Cisco CallManager service. If the problem persists, contact the Cisco Technical Assistance Center (TAC).
32	DeviceTypeMismatch - The device type reported by the device does not match the device type configured on Unified CM. Verify that the Product Type on the Phone Configuration page in Unified CM Administration matches the model number of the phone. If it does not match, delete the phone and add a new one with the correct Product Type. If the device is a Cisco phone, verify that the TFTP service is running and reachable by the phone, and view the Unified CM Database Status report in Cisco Unified Reporting to verify that database replication is Good. You can also issue the following command on the CLI to view database repliction: utils dbreplication runtimestate.
33	AddressingModeMismatch - (SCCP only) 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; or 2) The device is configured to use only IPv6 addressing, but did not specify an IPv6 address. Reset the device to resolve the problem. If the problem persists, restart the Cisco CallManager service.
34	SourceVerificationForSoftwareMediaDevicesFailure – This applies to Annunciator (ANN) and Music on Hold (MOH) servers only. When the enterprise parameter Cluster Security Mode is set to 1 (mixed mode) and the Unified CM service parameter Enable Source Verification for Software Media Devices is set to True, the source IP address of an ANN or MOH server will be verified to be one of the Unified CM nodes in the cluster. When this alarm occurs with value 34 as the reason, it means that the IP address of the ANN or MOH server is not a recognized node in the cluster. Because ANN or MOH servers currently can only be installed on a Unified CM node, an unknown server that registers an untrusted device as an ANN or MOH server could indicate a security breach. The IP address of the device trying to register is included as part of the alarm; use the IP address to determine whether an unapproved server is attempting to register or if a network address translation (NAT) error occurred because a firewall device is in the network path between two Unified CM nodes.
35	AuthorizationError – (SIP devices only) Device registration failed due to one of the following reasons: 1) userid in the Contact header of SIP REGISTER message does not match with any of the configured values in Unified CM (Owner User ID in phone configuration page and User ID associated with the device in EndUser page); or 2) If there are more than one userid present in the Contact header of SIP REGISTER message, that is considered as a security risk. Check the CUCM configuration as mentioned above to see whether authorized user is trying to register this particular device.

Enum Definitions – IPAddrAttributes

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

Enum Definitions - IPV6AddrAttributes

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

Error Message

%UC_CALLMANAGER-3-EndPointTransientConnection: %[IPAddress=String][DeviceName=String][MACAddress=String][Protocol=String][DeviceType=Enum][Reason=Enum][ConnectingPort=UInt][SIPUser=String][IPV6Address=String][IPAddrAttributes=Enum][IPV6AddrAttributes=Enum][LastSignalReceived=String][StationState=String][AppID=String][ClusterID=String][NodeID=String]: An endpoint attempted to register but did not complete registration.

Explanation 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.

Recommended Action Investigate any network connectivity problems in the system. It's possible that you have reached the maximum number of devices; the Cisco CallManager service parameter, Maximum Number of Registered Devices, controls the number of devices allowed in the system. After 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 in the alarm for additional recommended actions. No action is required if this event was issued as a result of a normal device rehome.

Reason Code - Enum Definitions

Enum Definitions - DeviceType

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

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
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

Enum Definitions - Reason

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 the Cisco Technical Assistance Center (TAC).
2	NoEntryInDatabase - (MGCP only) The device is not configured in the 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 in Cisco Unified CM Administration.
3	DatabaseConfigurationError - The device is not configured in the 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 in Cisco 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 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 that "all servers have a good replication status." If DB replication looks good, reset the phone. If resetting the phone doesn't fix the issue, restart TFTP and Cisco CallManager services. For all other devices, this reason code means that DNS lookup failed. Verify that 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 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 Unified CM node is

	experiencing high CPU usage. Verify that the device is powered up and operating, verify network connectivity between the device and Unified CM, and verify that the CPU utilization is in the safe range (you can monitor this via the CPU Pegging Alert in RTMT).
7	InitializationError - An internal error occurred within Unified CM while processing the device registration. Cisco recommends that you restart the Cisco CallManager service. If this issue 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 the Cisco Technical Assistance Center (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 (System > Security Profile > Phone Security Profile, check whether the Enable Digest Authentication checkbox is checked), verify that the Digest Credentials field in the End User Configuration page is configured. Also, check the Phone Configuration page to determine whether the phone is associated with the specified end user in the Digest User drop-down list box. If the device is a third-party SIP device, verify that the digest credentials configured on the phone match the Digest

	Credentials configured in the End User Configuration page in Unified CM Administration.
11	InvalidX509NameInCertificate – The configured X.509 Subject Name doesn't match the information in the certificate from the device. Check the Security profile of the indicated device and verify that the Device Security Mode is set to either Authenticated or Encrypted. Verify that the X.509 Subject Name field has the appropriate information. It should match the Subject Name in the certificate from the peer.
12	InvalidTLSCipher – An unsupported cipher algorithm was used by the device; 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, or an expires value that is too small. Check the REGISTER message for any of these issues and if you find one, correct the issue.
15	ProtocolMismatch – The protocol of the device (SIP or SCCP) does not match the configured protocol in Unified CM. Recommended actions: 1) Verify that the device is configured with the desired protocol; 2) Verify that the firmware load ID on the Device

	Defaults page in Unified CM Administration is correct and actually exists on the TFTP server; 3) If there is a firmware load ID configured on the device page, verify that it is correct and exists on the TFTP server (on the Cisco Unified OS Administration page, access Software Upgrades > TFTP File Management, then 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 that 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 the Cisco Technical Assistance Center (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 Configuration page, verify that the

	firmware load ID exists on the TFTP server (on the Cisco Unified OS Administration page, access Software Upgrades > TFTP File Management, then look for the file name as specified by load ID).
19	DigestAuthChallenge – (SIP only) A SIP device configured for digest authentication attempted to register with invalid credentials. Unified CM has responded with a challenge (401) to request new credentials.
20	DigestAuthChallengeForID – (SIP only) A SIP device attempted to register without a device name or MAC address. Unified CM responded with a challenge (401) which requests the device to resend the REGISTER message and include an Authorization header containing a user ID. Unified CM will use this user ID to attempt to find the device in the configuration database.
21	DigestChallengeTimeout – (SIP only) A SIP device requiring digest authentication sent a REGISTER message and Unified CM responded with a challenge (401) to request the authorization credentials. The device did not resend the REGISTER within the 30-second timeout interval.
22	ExpiresTimeTooSmall – (SIP only) A SIP device attempted to register with an Expires value smaller than the configured SIP Station Keepalive Interval value in the Call Manager Service Parameters. Unified CM responded with 423 Interval Too Brief and the device

	should re-register with the correct Expires value.
23	DatabaseTimeout - Unified CM requested device configuration data from the database but did not receive a response in time (within 15 seconds for SIP devices, or within 10 minutes for SCCP devices).
24	UniqueDeviceForUserNotFound - (SIP only) A 3rd-party device attempted to register but there is more than 1 device associated with the same Digest User. Third-party devices must be configured with a unique Digest User.
25	RegistrationSequenceError - (SCCP only) A device requested configuration information from Unified CM at an unexpected time and Unified CM had not yet obtained the requested information. The device will automatically attempt to register again. If this alarm occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be an internal firmware error. Collect existing SDI and SDL traces and contact the Cisco Technical Assistance Center (TAC).
26	InvalidCapabilities - (SCCP only) Unified CM detected an error in the media capabilities reported in the StationCapabilitiesRes message by the device during registration. The device will automatically attempt to register again. If this alarm occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be a

	protocol error. Collect existing SDI and SDL traces and contact the Cisco Technical Assistance Center (TAC).
27	CapabilityResponseTimeout – (SCCP only) Unified CM timed out while waiting for the device to respond to a request to report its media capabilities. 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 that the device is powered up and operating, verify that network connectivity exists between the device and Unified CM, and verify that the CPU utilization is in the safe range (you can monitor this via the CPU Pegging Alert in RTMT).
28	SecurityMismatch – Unified CM detected a mismatch in the security settings of the device and/or Unified CM. This alarm can occur due to any of the following situations: The device established a secure connection yet reported that it does not have the ability to do authenticated signaling; the device did not establish a secure connection but the security mode configured for the device indicates that it should have done so; or the device established a secure connection but the security mode configured for the device indicates that it should not have done so. To correct the error, ensure that the

	security settings of the device and Unified CM are correct for your deployment. Resetting the device may help because it forces the device to download its latest settings. If the device is a Cisco phone, verify that the TFTP service is running and reachable by the phone and view the Unified CM Database Status report in Cisco Unified Reporting to verify that database replication is Good. You can also issue the following command on the CLI to view database replication: utils dbreplication runtimestate. If the device is a third-party SIP phone, verify that the configuration on the phone is set to UDP or TCP only; Unified CM does not support TLS on third-party phones. Because each third-party phone model has unique configuration interfaces, please refer to the configuration guide for your phone to learn where the third-party phone defines the UDP/TCP setting.
29	AutoRegisterDBError - Auto-registration of a device failed because auto-registration is not allowed for the device type or because an error occurred while adding the auto-registering device to the database (stored procedure). Note that if Unified CM is in mixed mode (System > Enterprise Parameters > Cluster Security Mode = 1), auto-registration is not allowed and the device must be configured manually. If you are not planning to auto-register phones, either manually configure the phone (Device > Phone > Add New),

	power the device down, or remove it from the network. If you are attempting to auto-register this phone, verify that the cluster is not in mixed mode (System > Enterprise Parameters > Cluster Security Mode = 1) and verify that auto-registration is enabled on the node to which this device is registering (System > Cisco Unified CM > ensure that the Auto-registration Disabled... checkbox is not checked).
30	DBAccessError - Device registration failed because of an error that occurred while building the station registration profile. This usually indicates a synchronization problem with the database. View the Unified CM Database Status report in Cisco Unified Reporting to verify that database replication is Good. You can also issue the following command on the CLI to view database replication: utils dbreplication runtimestate. When database replication is Good on all nodes, restart the Cisco CallManager service on the node to which the device is attempting to register. If the problem persists, collect SDI and SDL traces for the Cisco Database layer Monitor service and contact the Cisco Technical Assistance Center (TAC).
31	AutoRegisterDBConfigTimeout - (SCCP only) 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. The device will automatically attempt

	to register again. Check for high CPU utilization on this Unified CM node because congestion could be a cause of this alarm. If this alarm continues to occur, restart the Cisco CallManager service. If the problem persists, contact the Cisco Technical Assistance Center (TAC).
32	DeviceTypeMismatch – The device type reported by the device does not match the device type configured on Unified CM. Verify that the Product Type on the Phone Configuration page in Unified CM Administration matches the model number of the phone. If it does not match, delete the phone and add a new one with the correct Product Type. If the device is a Cisco phone, verify that the TFTP service is running and reachable by the phone, and view the Unified CM Database Status report in Cisco Unified Reporting to verify that database replication is Good. You can also issue the following command on the CLI to view database repliction: utils dbreplication runtimestate.
33	AddressingModeMismatch – (SCCP only) 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; or 2) The device is configured to use only IPv6 addressing, but did not specify an IPv6 address. Reset the device to resolve the problem. If the

	problem persists, restart the Cisco CallManager service.

Enum Definitions - IPAddrAttributes

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

Enum Definitions - IPV6AddrAttributes

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

Error Message

%UC_CALLMANAGER-6-DeviceRegistered: %[DeviceName=String][{Optional}MACAddress=String] [{Optional}IPAddress=String][Protocol=String][{Optional}Description=String][{Optional}UserID=String] [{Optional}LoadID=String][{Optional}AssociatedDNs=String][PerfMonObjType=Enum] [{Optional}DeviceType=Enum][{Optional}ConfigGKName=String][{Optional}TechPrefix=String] [{Optional}Zone=String][{Optional}AltGKList=String][{Optional}ActiveGK=String] [{Optional}CallSignalAddr=String][{Optional}RASAddr=String][{Optional}IPV6Address=String] [{Optional}IPAddrAttributes=Enum][{Optional}IPV6AddrAttributes=Enum] [{Optional}ActiveLoadId=String][{Optional}InactiveLoadId=String][AppID=String][ClusterID=String] [NodeID=String]: Device registered.

Explanation A device successfully registered with Cisco Unified Communications Manager

Recommended Action Informational purposes only; no action is required

Reason Code - Enum Definitions

Enum Definitions - PerfMonObjType

Value	Definition
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
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
33	External Call Control
34	Cisco SAF Client
35	IME Client
36	IME Client Instance

Enum Definitions - DeviceType

Value	Definition
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
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
254	UNKNOWN_MGCP_GATEWAY
255	UNKNOWN
30027	ANALOG_PHONE
30028	ISDN_BRI_PHONE
30032	SCCP_GATEWAY_VIRTUAL_PHONE

Enum Definitions - IPAddrAttributes

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

Enum Definitions - IPV6AddrAttributes

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

Error Message

%UC_CALLMANAGER-6-EndPointRegistered: %[DeviceName=String][MACAddress=String] [IPAddress=String][Protocol=String][Description=String][UserID=String][LoadID=String] [AssociatedDNs=String][PerfMonObjType=Enum][DeviceType=Enum][IPV6Address=String] [IPAddrAttributes=Enum][IPV6AddrAttributes=Enum][ActiveLoadId=String][InactiveLoadId=String] [AppID=String][ClusterID=String][NodeID=String]: Endpoint registered.

Explanation An endpoint successfully registered with Cisco Unified Communications Manager

Recommended Action Notification purposes only; no action is required

Reason Code - Enum Definitions

Enum Definitions - PerfMonObjType

Value	Definition
2	Cisco Phone

Enum Definitions - DeviceType

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
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
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

Enum Definitions - IPAddrAttributes

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

Enum Definitions - IPV6AddrAttributes

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

Error Message

%UC_CALLMANAGER-4-DevicePartiallyRegistered: %[DeviceName=String] [{Optional}MACAddress=String][IPAddress=String][Protocol=String][{Optional}Description=String] [{Optional}UserID=String][{Optional}LoadID=String][AssociatedDNs=String][PerfMonObjType=Enum]

[{Optional}DeviceType=Enum][ActiveLoadId=String][InactiveLoadId=String][IPV6Address=String][AppID=String][ClusterID=String][NodeID=String]: A device has partially registered.

Explanation A device is partially registered with Cisco Unified Communications Manager. Some, but not all, of the lines configured on the device have successfully registered.

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-Line 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.

Reason Code - Enum Definitions

Enum Definitions - PerfMonObjType

Value	Definition
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
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
33	External Call Control
34	Cisco SAF Client
35	IME Client
36	IME Client Instance

Enum Definitions - DeviceType

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
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
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
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
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
30019	CISCO_7936
30027	ANALOG_PHONE
30028	ISDN_BRI_PHONE
30032	SCCP_GATEWAY_VIRTUAL_PHONE
30035	IP_STE

Error Message

%UC_CALLMANAGER-4-DeviceUnregistered: %[DeviceName=String][{Optional}MACAddress=String] [{Optional}IPAddress=String][Protocol=String][{Optional}DeviceType=Enum] [{Optional}Description=String][{Optional}Reason=Enum][{Optional}IPV6Address=String] [{Optional}IPAddrAttributes=Enum][{Optional}IPV6AddrAttributes=Enum][AppID=String] [ClusterID=String][NodeID=String]: Device unregistered.

Explanation A device that has previously registered with Unified CM 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, and 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 coming online, which causes 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.

Recommended Action Actions to take vary depending on the reason specified in this alarm 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 problem or loss of KeepAlives, 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.

Reason Code - Enum Definitions

Enum Definitions - DeviceType

Value	Definition
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
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
254	UNKNOWN_MGCP_GATEWAY
255	UNKNOWN
30027	ANALOG_PHONE
30028	ISDN_BRI_PHONE
30032	SCCP_GATEWAY_VIRTUAL_PHONE

Enum Definitions - Reason

Value	Definition
1	Unknown - The device has unregistered for an unknown reason. If the device does not re-register within 5 minutes, verify that it is powered up and verify that there is network connectivity between the device and Unified CM.
6	ConnectivityError - Network communication between the device and 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 Unified CM node is experiencing high CPU usage.

	Verify that the device is powered up and operating, verify that there is network connectivity between the device and Unified CM, and verify that the CPU utilization is in the safe range (you can monitor this via the CPU Pegging Alert in RTMT).
8	DeviceInitiatedReset - The device has initiated a reset, possibly due to a power cycle or internal error. No action required; the device will re-register 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 re-register 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 re-register 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, or an expires value that is too small. Check the REGISTER message for any of these

	issues and if you find one, correct the issue.
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 Unified CM node is experiencing high CPU usage. Verify that the device is powered up and operating, verify that there is network connectivity between the device and Unified CM, and verify the CPU utilization is in the safe range (you can

	monitor this via the CPU Pegging Alert in RTMT).
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. Go to the Cisco Unified Reporting web page, generate a Unified CM Database Status report and verify "all servers have a good replication status". You can also go to the Real-Time Reporting Tool (RTMT) and check the Replication Status in the Database Summary page. If status shows 2, then replication is working. If this device continues to unregister with this reason code, go to the Device Configuration page in Unified CM Administration for the device indicated in this alarm and click Save. This generates a change notify message to the Cisco CallManager and TFTP services and rebuilds a new configuration file for the device. If the problem still persists, restart the TFTP service and the Cisco CallManager service.
15	CallManagerRestart - A device restart was initiated from Unified CM Administration, either due to an explicit command from an administrator or due to a configuration change such as adding, deleting or changing a

	directory number associated with the device. No action is necessary; the device will re-register automatically.
16	DuplicateRegistration - Unified CM detected that the device attempted to register to two nodes at the same time. Unified CM initiated a restart to the phone to force it to re-home to a single node. No action is necessary; the device will re-register automatically.
17	CallManagerApplyConfig - An ApplyConfig action was performed in Unified CM Administration resulting in an unregistration. No action is necessary; the device will re-register 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 re-register within 5 minutes, confirm that it is powered up and confirm that there is network connectivity between the device and 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
25	RegistrationSequenceError - (SCCP only) A device requested configuration information from Unified CM at

	an unexpected time and Unified CM no longer had the requested information in memory. The device will automatically attempt to register again. If this alarm occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be an internal firmware error. Collect existing SDI and SDL traces and contact the Cisco Technical Assistance Center (TAC).
26	InvalidCapabilities - (SCCP only) Unified CM detected an error in the updated media capabilities reported in one of the StationUpdateCapabilities messages sent by the device. The device will automatically attempt to register again. If this alarm occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be a protocol error. Collect existing SDI and SDL traces and contact the Cisco Technical Assistance Center (TAC).
28	FallbackInitiated - The device has initiated a fallback and will automatically re-register to a higher-priority Unified CM. No action is necessary.

Enum Definitions - IPAddrAttributes

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

Enum Definitions – IPV6AddrAttributes

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

Error Message

%UC_CALLMANAGER-3-EndPointUnregistered: %[DeviceName=String][MACAddress=String] [IPAddress=String][Protocol=String][DeviceType=Enum][Description=String][Reason=Enum] [IPV6Address=String][IPAddrAttributes=Enum][IPV6AddrAttributes=Enum]

[LastSignalReceived=String][CallState=String][AppID=String][ClusterID=String][NodeID=String]: An endpoint has unregistered.

Explanation 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 coming online, causing the phone to rehome to the primary Unified CM node. Or, lack of a KeepAlive message being returned from the Unified CM node to which this endpoint was registered. Unregistration also occurs if Unified CM receives a duplicate registration request for this same device.

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 problem or loss of KeepAlives, 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 in this alarm for additional recommended actions.

Reason Code - Enum Definitions

Enum Definitions - DeviceType

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
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
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

Enum Definitions - Reason

Value	Definition
1	Unknown - The device has unregistered for an unknown reason. If the device does not re-register within 5 minutes, verify that it is powered up and verify that network connectivity exists between the device and Unified CM.
6	ConnectivityError - Network communication between the device and 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 Unified CM node is experiencing high CPU usage.

	Verify that the device is powered up and operating, verify that network connectivity exists between the device and Unified CM, and verify that the CPU utilization is in the safe range (you can monitor this via the CPU Pegging Alert in RTMT).
8	DeviceInitiatedReset - The device has initiated a reset, possibly due to a power cycle or internal error. No action is required; the device will re-register automatically.
9	CallManagerReset - A device was reset from Cisco Unified CM Administration, either due to an explicit command from an administrator, or due to internal errors encountered. No action is necessary; the device will re-register 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 re-register 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, or an expires value that is too small. Check the REGISTER message for any of these issues and if you find one, correct the issue.

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 is necessary; the device will re-register 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 that the device is powered up and operating, verify that network connectivity exists between the device and Unified CM, and verify that the CPU utilization is in the safe range (you can monitor this via the CPU Pegging Alert in

	RTMT). No action is necessary; the device will re-register 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". You can also go to the Real-Time Reporting Tool (RTMT) and check the Replication Status in the Database Summary page. If status shows 2, then replication is working. If this device continues to unregister with this reason code, go to the Device Configuration page in Unified CM Administration for the device identified in this alarm and click Save. This generates a change notification message to the Cisco CallManager and TFTP services and rebuilds a new configuration file. If the problem still persists, restart the TFTP service and Cisco CallManager service.
15	CallManagerRestart - A device restart was initiated from Unified CM, either due to an explicit command from an administrator, or due to a configuration change such as adding, deleting or changing a directory number associated

	with the device. No action is necessary; the device will re-register automatically.
16	DuplicateRegistration - Unified CM detected that the device attempted to register to two nodes at the same time. Unified CM initiated a restart to the phone to force it to re-home to a single node. No action is necessary; the device will re-register automatically.
17	CallManagerApplyConfig - An ApplyConfig action was performed in Unified CM Administration resulting in an unregistration. No action is necessary; the device will re-register 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 re-register within 5 minutes, confirm that the device is powered-up and confirm that network connectivity exists between the device and 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 re-registered. 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 Unified CM at an unexpected time and Unified CM no longer had the requested information in memory. The device will automatically attempt to register again. If this alarm

	occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be an internal firmware error. Collect existing SDI and SDL traces and contact the Cisco Technical Assistance Center (TAC).
26	InvalidCapabilities - (SCCP only) Unified CM detected an error in the updated media capabilities reported in one of the StationUpdateCapabilities messages sent by the device. The device will automatically attempt to register again. If this alarm occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be a protocol error. Collect existing SDI and SDL traces and contact the Cisco Technical Assistance Center (TAC).
28	FallbackInitiated - The device has initiated a fallback and will automatically re-register 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.
30	DeviceWipe - An administrator has reset this device to factory settings. All configuration and data on the device will be erased. This device may remain unregistered until reconfigured.

31	DeviceForcedReset – The device has been reset to resolve an inconsistency issue caused by a network connectivity problem. This forced reset is triggered by a SIP 503 response to a SIP Register message. The endpoint should automatically retry the SIP registration after this reset.
33	LowBattery – The device initiated a graceful shutdown due to battery depletion.
34	ManualPowerOff – The device unregistered because it was manually powered off.

Enum Definitions – IPAddrAttributes

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

Enum Definitions – IPV6AddrAttributes

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

Error Message

%UC_CALLMANAGER-4-SIPLineRegistrationError: %[IPAddress=String][DevicePort=UInt] [{Optional}DeviceName=String][{Optional}MACAddress=String][{Optional}DeviceType=Enum] [{Optional}Reason=Enum][ConnectingPort=UInt][ConfiguredDNs=String][SIPUser=String] [IPV6Address=String][AppID=String][ClusterID=String][NodeID=String]: SIP line registration error.

Explanation A SIP line attempted to register with Cisco Unified Communications Manager (Unified CM) 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. This alarm typically occurs with a third-party device.

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. To do so, 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. Refer to the reason code definitions for additional recommended actions.

Reason Code - Enum Definitions

Enum Definitions - DeviceType

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
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
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

Enum Definitions - Reason

Value	Definition
2	MisconfiguredDirectoryNumber - There is a configuration mismatch between the directory numbers configured on the phone and the directory numbers configured in the

	Unified CM database. If this is a third-party phone, confirm that the phone configuration is correct and matches the Unified CM configuration. If this is a Cisco IP phone, go to the Cisco Unified Reporting web page and confirm that database replication has a "good status" in the Unified CM Database Status report. 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. If the database replication status is good, reset the device. If the problem still persists, restart the TFTP service and the Cisco CallManager service from the Control Center - Feature Services web page.
3	MalformedRegisterMessage - 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.
4	AuthenticationError - The digest User ID or password sent from the phone does not match the User ID or password configured in Cisco Unified CM Administration. Digest User ID is the end user who is associated with the phone, as shown on the Phone Configuration page (in the Digest User drop-down list

	box). Password is configured on the End User Configuration page in the Digest Credentials field. If this is a third-party phone, ensure that the phone's digest credentials match the digest credentials configured on the End User Configuration page in Unified CM Administration. If this is a Cisco IP phone, go to the Cisco Unified Reporting web page to confirm that database replication has a "good status" in the Unified CM Database Status report. 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. If the database replication status is good, reset the device. If the problem still persists, restart the TFTP service and the Cisco CallManager 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 on the phone's Device Configuration page in Unified CM Administration. If the device is a Cisco phone, go to the Cisco Unified Reporting web page to confirm that database replication has a "good status" in the Unified CM Database Status report. 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. If the database replication status is good, reset the device. If the problem still persists, restart the TFTP service and the Cisco CallManager service from the Control Center - Feature Services web page.
8	BulkRegistrationError - An 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 service turned on and contact the Cisco Technical Assistance Center (TAC).

Error Message

%UC_CALLMANAGER-5-H323Started: %[DeviceName=String][IPAddress=String] [{Optional}DeviceType=Enum][{Optional}Description=String] [{Optional}RemoteUnifiedCMServerList=String][AppID=String][ClusterID=String] [NodeID=String]: Unified CM is ready to handle calls for the indicated H.323 device.

Explanation Cisco Unified Communications Manager (Unified CM) 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).

Recommended Action Notification purposes only; no action is required

Reason Code - Enum Definitions

Enum Definitions - DeviceType

Value	Definition
61	H323_PHONE
62	H323_GATEWAY
122	GATEKEEPER
125	TRUNK

Error Message

%UC_CALLMANAGER-4-H323Stopped: %[DeviceName=String][IPAddress=String] [{Optional}DeviceType=Enum][{Optional}Description=String][AppID=String][ClusterID=String] [NodeID=String]: Unified CM is not ready to handle calls for the indicated H.323 device.

Explanation 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.

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.

Reason Code - Enum Definitions

Enum Definitions - DeviceType

Value	Definition
61	H323_PHONE
62	H323_GATEWAY
122	GATEKEEPER
125	TRUNK

Error Message

%UC_CALLMANAGER-5-SIPStarted: %[DeviceName=String][{Optional}IPAddress=String] [{Optional}DeviceType=Enum][{Optional}Description=String][InPortNbr=UInt][OutPortNbr=UInt]

[InTransportType=Enum][OutTransportType=Enum][{Optional}IPV6Address=String][AppID=String] [ClusterID=String][NodeID=String]: Unified CM is ready to handle calls for the indicated SIP device.

Explanation Unified CM is ready to handle calls for the indicated SIP device. This alarm does not indicate the current state of the SIP device, only that Unified CM is prepared to handle calls to/from the SIP device.

Recommended Action Informational purposes only; no action is required

Reason Code - Enum Definitions

Enum Definitions - DeviceType

Value	Definition
131	SIP_TRUNK

Enum Definitions - InTransportType

Value	Definition
1	TCP
2	UDP
3	TLS
4	TCP/UDP

Enum Definitions - OutTransportType

Value	Definition
1	TCP
2	UDP
3	TLS

Error Message

%UC_CALLMANAGER-4-SIPStopped: %[DeviceName=String][IPAddress=String] [{Optional}DeviceType=Enum][{Optional}Description=String][InPortNbr=UInt][OutPortNbr=UInt] [InTransportType=Enum][OutTransportType=Enum][{Optional}IPV6Address=String][AppID=String] [ClusterID=String][NodeID=String]: Unified CM is not ready to handle calls for the indicated SIP device.

Explanation Unified CM 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 Cisco Unified CM Administration.

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.

Reason Code - Enum Definitions

Enum Definitions - DeviceType

Value	Definition

131	SIP_TRUNK

Enum Definitions - InTransportType

Value	Definition
1	TCP
2	UDP
3	TLS
4	TCP/UDP

Enum Definitions - OutTransportType

Value	Definition
1	TCP
2	UDP
3	TLS

Error Message

%UC_CALLMANAGER-5-SIPNormalizationScriptOpened: %[DeviceName=String][ScriptName=String][InUseMemory=UInt][AppID=String][ClusterID=String][NodeID=String]: Unified CM has opened the script for this device.

Explanation The normalization script for the indicated SIP device has been successfully loaded, initialized, and is active on Unified CM

Recommended Action Notification purposes only; no action is required

Error Message

%UC_CALLMANAGER-5-SIPNormalizationScriptClosed: %[DeviceName=String][ScriptName=String][ReasonCode=Enum][ReasonText=String][AdditionalInformation=String][AppID=String][ClusterID=String][NodeID=String]: Unified CM has closed (disabled) the script for this device .

Explanation Unified CM closed the script either because the indicated device (SIP trunk) was reset manually or automatically, the trunk was deleted, or because of a script error or resource error, or because of an internal error. When the script is closed, Unified CM is not invoking normalization script message handlers for the indicated SIP device.

Recommended Action This alarm serves as notification of the script closure if the alarm occurred due to a SIP trunk maintenance window or some 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 that alarm.

Reason Code - Enum Definitions

Enum Definitions - ReasonCode

Value	Definition
1	DeviceResetManually - The associated device was

	manually reset via Cisco Unified CM Administration
2	DeviceResetAutomatically – The associated device was reset automatically; the reset was triggered by an execution error in the script
3	DeviceDeleted – The associated device was 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 a SIPNormalizationScriptError alarm and perform the recommended actions described to correct the script error

Error Message

%UC_CALLMANAGER-3-SIPNormalizationScriptError: %[DeviceName=String][ScriptName=String] [ScriptFunction=String][ScriptType=String][ErrorCode=Enum][ErrorCodeText=String] [ErrorMessage=String][ConfiguredAction=String][ResultingAction=String][InUseMemory=UInt] [MemoryThreshold=UInt][InUseLuaInstructions=UInt][LuaInstructionThreshold=UInt][AppID=String] [ClusterID=String][NodeID=String]: A script error occurred.

Explanation 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, 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.

Recommended Action Examine SDI trace files for details regarding the error such as function calls and the call ID which may help provide details that assist with troubleshooting 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 that alarm for additional information and recommended actions.

Reason Code - Enum Definitions

Enum Definitions - ErrorCode

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

Error Message

%UC_CALLMANAGER-3-SIPNormalizationResourceWarning: %[DeviceName=String] [ScriptName=String][ScriptFunction=String][ScriptType=String][ReasonCode=Enum] [ReasonText=String][InUseMemory=UInt][MemoryThreshold=UInt][InUseLuaInstructions=UInt] [LuaInstructionThreshold=UInt][AppID=String][ClusterID=String][NodeID=String]: The script has exceeded an internal resource threshold and may be in danger of closing.

Explanation 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. For example, 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 Unified CM release to release. Another example: if the Lua Instruction Threshold is set to 2000 and the internal threshold is 50%, this alarm occurs when the script has executed 1000 Lua instructions. This alarm serves as a warning that resources (either memory or Lua instructions) have passed an internal mark where investigation into the consumption of those resources may be advisable to ensure the health of the script. Investigate and correct the resource issue before the script closes. When the values that have been configured in the fields, Memory Threshold field and/or Lua Instruction Threshold 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.

Recommended Action Examine the thresholds (Memory Threshold and Lua Instruction Threshold) configured in the SIP Normalization Script Configuration window and evaluate if those 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. Examine the script for logic errors. If the script is otherwise 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).

Reason Code - Enum Definitions

Enum Definitions - ReasonCode

Value	Definition
1	InternalLuaInstructionsThreshold - The script exceeded the internal threshold for the number of Lua instructions
2	InternalMemoryThreshold - The script exceeded the internal threshold for script memory usage

Error Message

%UC_CALLMANAGER-5-SIPNormalizationAutoResetDisabled: %[DeviceName=String] [ScriptName=String][ScriptType=String][ReasonCode=Enum][ReasonText=String] [AdditionalInformation=String][AppID=String][ClusterID=String][NodeID=String]: An error has occurred repeatedly and Unified CM disabled the script.

Explanation The script failed due to execution errors three times within a 10 minute period. As a result, the normalization script for the indicated SIP device has been disabled. Unified CM is no longer attempting to automatically reset either the script or the device for the purposes of recovering the script.

Recommended Action Notification purposes; examine the information and perform the recommended actions in the SIPNormalizationScriptError alarm, which should have been issued prior

to this alarm

Reason Code - Enum Definitions

Enum Definitions - ReasonCode

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, 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, Unified CM disabled the script

Error Message

%UC_CALLMANAGER-5-SIPTrunkISV: %[DeviceName=String][AvailableRemotePeers=String] [AppID=String][ClusterID=String][NodeID=String]: All remote peers are available to handle calls for this SIP trunk .

Explanation All remote peers are available to handle calls for this SIP trunk. This alarm specifies the available remote peers for this SIP trunk; each peer is identified by resolved IP address and port number, and hostname or SRV if configured on SIP trunk.

Recommended Action Notification purpose only; no action is required

Error Message

%UC_CALLMANAGER-3-SIPTrunkOOS: %[DeviceName=String] [UnavailableRemotePeersWithReasonCode=String][AppID=String][ClusterID=String] [NodeID=String]: All remote peers are out of service and unable to handle calls for this SIP trunk.

Explanation All remote peers for this SIP trunk are out of service and unable to handle calls. This alarm provides the reason code received by the SIP trunk in response to an Options request sent to the remote peer. The list of unavailable remote peers is provided in this alarm and each peer is separated by semi-colon. 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. ReasonCodeType could be based on a SIP response from the remote peer as defined in SIP RFCs (Remote) or based on a reason code provided by Unified CM (Local). 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 not able to create a socket connection with the remote

peer), Local=3 (DNS query failed). For Local=3, IP address in Alarm will be represented as "0" and when dns srv is configured on SIP trunk then port will be represented as "0".

Recommended Action For Remote=503, possible reasons include 1) route/sip trunk for originating side doesn't exist on remote peer; 2) route/sip trunk for originating side does exist on the remote peer but the port is either used for a SIP phone or a different sip trunk; 3) the remote peer has limited resources and may not be able to handle new calls. For the first cause (item 1), if the remote peer is Unified CM, add a new SIP trunk in Unified CM Administration for the remote peer (Device > Trunk) and make certain that 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 same as originating side SIP Trunk destination port. For the second cause (item 2), if the remote peer is Unified CM, then in Unified CM Administration for the remote peer (Device > Trunk) make certain that incoming port in associated SIP Trunk Security Profile is configured to be same as originating side SIP Trunk destination port. For the third cause (item 3), if the remote peer is administered by a different system administrator, consider communicating the resource issue with the other administrator. For remote=408, possible reason includes remote is running low in resources and unable to process the request. If the remote peer is administered by a different system administrator, consider communicating the resource issue with the other administrator. For Local=1, possible reason could be that no responses has been received for Options request after all retries when transport is configured as UDP in SIP trunk Security Profile assigned to the SIP trunk on originating side. To fix this issue, if the remote peer is Unified CM, then go to remote peer Serviceability web page and then Tools -> Control Center (Feature Services) and make sure Cisco Call Manager service is activated and started. Also, go to remote peer admin web page and then to Device -> Trunk and do a find and make sure that there is a SIP trunk exist with incoming port in associated SIP Trunk security profile configured to be same as what is configured on originating side SIP Trunk destination port. Also, check the network connectivity using the CLI command "utils network ping remote_peer" at originating side. For Local=2, possible reason could be that Unified CM is not be able to create socket connection with remote peer. To fix this issue, if remote peer is Unified CM, then go to remote peer Serviceability web page and then Tools -> Control Center (Feature Services) and make sure Cisco Call Manager service is activated and started. Also, go to remote peer admin web page and then to Device -> Trunk and do a find and make sure that there is a SIP trunk exist with incoming port in associated SIP Trunk security profile configured to be same as what is configured on originating side SIP Trunk destination port. Also, check the network connectivity using "utils network ping remote_peer" at originating side. For Local=3, possible reason could be DNS server is not reachable or DNS is not properly configured to resolve hostname or SRV which is configured on local SIP trunk. To fix this issue, go to OS Administration web page and go to Show -> Network and look into DNS Details and make sure it is correct. If not then configure correct DNS server information using CLI "set network dns primary" command. Also, check the network connectivity with DNS server using "utils network ping "remote_peer" and make sure DNS server is properly configured.

Error Message

%UC_CALLMANAGER-4-SIPTrunkPartiallyISV: %[DeviceName=String] [UnavailableRemotePeersWithReasonCode=String][AvailableRemotePeers=String][AppID=String] [ClusterID=String][NodeID=String]: Some of the remote peers are not available to handle calls for this SIP Trunk.

Explanation Some of the remote peers are not available to handle calls for this SIP trunk. This alarm provides a list of available remote peers and a list of unavailable remote peers and each peer is separated by semi-colon. Each available peer is identified by resolved IP address and port number, and hostname or SRV (if configured on SIP trunk). In the case of unavailable peers, 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. ReasonCodeType could be based on a SIP

response from the remote peer as defined in SIP RFCs (Remote) or based on a reason code provided by Unified CM (Local). 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 not able to create a socket connection with the remote peer), Local=3 (DNS query failed). For Local=3, IP address in Alarm will be represented as "0" and when dns srv is configured on SIP trunk then port will be represented as "0".

Recommended Action Available peer list is for notification purpose only; no action is required. For each unavailable peer, complete the following steps depending on the reason code provided in this alarm. For Remote=503, possible reasons include 1) route/sip trunk for originating side doesn't exist on remote peer; 2) route/sip trunk for originating side does exist on the remote peer but the port is either used for a SIP phone or a different sip trunk; 3) the remote peer has limited resources and may not be able to handle new calls. For the first cause (item 1), if the remote peer is Unified CM, add a new SIP trunk in Unified CM Administration for the remote peer (Device > Trunk) and make certain that 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 same as originating side SIP Trunk destination port. For the second cause (item 2), if the remote peer is Unified CM, then in Unified CM Administration for the remote peer (Device > Trunk) make certain that incoming port in associated SIP Trunk Security Profile is configured to be same as originating side SIP Trunk destination port. For the third cause (item 3), if the remote peer is administered by a different system administrator, consider communicating the resource issue with the other administrator. For remote=408, possible reason includes remote is running low in resources and unable to process the request. If the remote peer is administered by a different system administrator, consider communicating the resource issue with the other administrator. For Local=1, possible reason could be that no responses has been received for Options request after all retries when transport is configured as UDP in SIP trunk Security Profile assigned to the SIP trunk on originating side. To fix this issue, if the remote peer is Unified CM, then go to remote peer Serviceability web page and then Tools -> Control Center (Feature Services) and make sure Cisco Call Manager service is activated and started. Also, go to remote peer admin web page and then to Device -> Trunk and do a find and make sure that there is a SIP trunk exist with incoming port in associated SIP Trunk security profile configured to be same as what is configured on originating side SIP Trunk destination port. Also, check the network connectivity using the CLI command "utils network ping remote_peer" at originating side. For Local=2, possible reason could be that Unified CM is not be able to create socket connection with remote peer. To fix this issue, if remote peer is Unified CM, then go to remote peer Serviceability web page and then Tools -> Control Center (Feature Services) and make sure Cisco Call Manager service is activated and started. Also, go to remote peer admin web page and then to Device -> Trunk and do a find and make sure that there is a SIP trunk exist with incoming port in associated SIP Trunk security profile configured to be same as what is configured on originating side SIP Trunk destination port. Also, check the network connectivity using "utils network ping remote_peer" at originating side. For Local=3, possible reason could be DNS server is not reachable or DNS is not properly configured to resolve hostname or SRV which is configured on local SIP trunk. To fix this issue, go to OS Administration web page and go to Show -> Network and look into DNS Details and make sure it is correct. If not then configure correct DNS server information using CLI "set network dns primary" command. Also, check the network connectivity with DNS server using "utils network ping "remote_peer" and make sure DNS server is properly configured.

Error Message

%UC_CALLMANAGER-3-ConnectionFailure: %[DeviceName=String][IPAddress=String] [{Optional}DeviceType=Enum][{Optional}Description=String][Reason=Enum][IPV6Address=String]

[AppID=String][ClusterID=String][NodeID=String]: Unified CM failed to open a TLS connection for the indicated device.

Explanation Unified CM failed to open a TLS connection for the indicated device because an incorrect Device Security Mode was configured or an incorrect X.509 Subject Name was configured, or due to an unsupported cipher algorithm

Recommended Action Check the Security Profile of the indicated device. Make certain that Device Security Mode is set to either Authenticated or Encrypted. Make sure that the X.509 Subject Name field has the appropriate content; it should match the Subject Name in the certificate from the peer. Also, Unified CM only supports the AES_128_SHA cipher algorithm; let the peer regenerate its certificate with the correct algorithm.

Reason Code - Enum Definitions

Enum Definitions - DeviceType

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
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
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

Enum Definitions - Reason

Value	Definition
1	AuthenticationError - Device Security Mode is not set to either Authenticated or Encrypted
2	InvalidX509NameInCertificate - Configured X.509 Subject Name doesn't match the name in the certificate from the peer
3	InvalidTLSCipher - Unsupported cipher algorithm used by the peer; Unified CM only supports AES_128_SHA

Error Message

%UC_CALLMANAGER-4-MediaResourceListExhausted: %[MediaResourceType=Enum] [MediaResourceListName=String][AppID=String][ClusterID=String][NodeID=String]: The requested device type is not found in the media resource list or default list or the configured devices are not registered.

Explanation 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

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; 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 determine 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 device is not configured in any of the Media Resource Groups of the Media Resource Group List for which the alarm is generated or in 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 that 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. All the devices of that type will display along with their status, device pool, and so on. Check the status field to see whether the device 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 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 actually 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.

Reason Code - Enum Definitions

Enum Definitions - MediaResourceType

Value	Definition
1	Media termination point

2	Transcoder
3	Conference bridge
4	Music On Hold
5	Monitor bridge
6	Recorder
7	Annunciator
8	Built-in bridge
9	RSVP agent

Error Message

%UC_CALLMANAGER-4-RouteListExhausted: %[RouteListName=String][AppID=String] [ClusterID=String][NodeID=String]: An available route could not be found in the indicated route list.

Explanation 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.

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.

Error Message

%UC_CALLMANAGER-4-HuntListExhausted: %[HuntListName=String][AppID=String] [ClusterID=String][NodeID=String]: An available line could not be found in the indicated hunt list.

Explanation An available line could not be found in the indicated hunt 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.

Recommended Action Consider adding additional lines in the indicated hunt list. Check whether there are some outstanding calls on the line. Try to make a call directly to the members, bypassing the hunt list, to verify that there is no 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.

Error Message

%UC_CALLMANAGER-3-DeviceTypeMismatch: %[DBDeviceType=Enum][DeviceType=Enum] [DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: Device type mismatch between the information contained in the device's TFTP configuration file and what is configured in Unified CM Administration for that device.

Explanation The device type indicated in the device's 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.

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.

Reason Code - Enum Definitions

Enum Definitions - DBDeviceType

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
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
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

Enum Definitions - DeviceType

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
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
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

Error Message

%UC_CALLMANAGER-6-DeviceDnInformation: %[DeviceName=String][{Optional}DeviceType=Enum][StationDesc=String][StationDn=String][AppID=String][ClusterID=String][NodeID=String]: List of directory numbers (DN) associated with this device.

Explanation Provides a list of directory numbers (DN) associated with the device

Recommended Action Informational purposes only; no action is required

Reason Code - Enum Definitions

Enum Definitions - DeviceType

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
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

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
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
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

Error Message

%UC_CALLMANAGER-6-StationConnectionError: %[DeviceName=String][ReasonCode=Enum] [AppID=String][ClusterID=String][NodeID=String]: Station device is closing the connection.

Explanation A station device is closing its connection with Unified CM because of the reason that is described in this alarm

Recommended Action Informational purposes only; no action is required. Also, refer to the reason code definition for additional information.

Reason Code - Enum Definitions

Enum Definitions - ReasonCode

Value	Definition
0	deviceInitiatedReset - The device has initiated a reset, possibly due to a power cycle or internal error. No action is required; the device will re-register automatically.
1	sccpDeviceThrottling - (SCCP only) The indicated SCCP device has 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 is required; the device will re-register 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 that the device is powered up and operating, verify network connectivity between the device and Unified CM, and verify that CPU utilization is in the safe range (you can monitor this via the CPU Pegging Alert in RTMT). No action is required; the device will re-register automatically.
3	dbChangeNotify - An ApplyConfig command was issued from Unified CM Administration resulting in an unregistration. No action is required; the device will re-register 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 re-registration should proceed normally. No action is required; the device will re-register automatically.
5	deepSleep - 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.
6	registrationSequenceError - (SCCP only) The device requested for a configuration information from the Unified CM at an unexpected time and the required information is no longer stored in the memory. No action is required; the device will re-register automatically.
7	invalidCapabilities - (SCCP only) Unified CM detected an error in the media capabilities reported in the StationCapabilitiesRes message by the device during registration. No action is required; the device will re-register automatically.
8	socketBroken - The TCP connection between the device and the Unified CM is broken. No action is required; the

	device will re-register automatically once the TCP connection is established.

Error Message

%UC_CALLMANAGER-6-StationAlarm: %[Protocol=String][TCPPid=String][DeviceText=String][Param1=UInt][Param2=UInt][AppID=String][ClusterID=String][NodeID=String]: A station has sent an alarm to Unified CM for pass-through purposes.

Explanation A station device sent an alarm to Unified CM, which acts as a conduit from the device to generate this alarm

Recommended Action To determine the appropriate action, refer to the specific device type and information passed from the device via this alarm

Error Message

%UC_CALLMANAGER-4-StationEventAlert: %[Protocol=String][TCPPid=String][DeviceText=String][Param1=UInt][Param2=UInt][AppID=String][ClusterID=String][NodeID=String]: A station sent an alert to Unified CM for pass-through purposes.

Explanation A station device sent an alert to Unified CM, which acts as a conduit from the device to generate this alarm

Recommended Action To determine the appropriate action, refer to the specific device type and information passed from the device via this alarm

Error Message

%UC_CALLMANAGER-5-MGCPGatewayGainedComm: %[DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: MGCP communication to the gateway has been established.

Explanation The MGCP gateway has established communication with Unified CM

Recommended Action Notification purposes only; no action is required

Error Message

%UC_CALLMANAGER-2-MGCPGatewayLostComm: %[DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: MGCP gateway has lost communication with Unified CM.

Explanation The MGCP gateway is no longer in communication with Unified CM. This could occur because Unified CM received an MGCP unregister signal from the gateway such as RSIP graceful/forced; Unified CM didn't receive the MGCP KeepAlive signal from the gateway; the MGCP gateway didn't response 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; or the gateway has reset.

Recommended Action Reset the MGCP gateway in an attempt to restore communication with 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.

Error Message

%UC_CALLMANAGER-2-StationPortInitError: %[AppID=String][ClusterID=String] [NodeID=String]: Station TCP initialization error.

Explanation An error during initialization was encountered

Recommended Action Verify that the Cisco Unified Communications Manager IP address is configured and is not configured as the loop back address for the IP version. Check the SCCP TCP port configuration to be sure the SCCP TCP port is accurately configured (be certain that there are no port conflicts where another port has the same number). If the IP and port settings are correct, collect SDL and SDI traces and contact the Cisco Technical Assistance Center (TAC).

Error Message

%UC_CALLMANAGER-3-DbInfoError: %[DeviceName=String][AppID=String][ClusterID=String] [NodeID=String]: Configuration information may be out of sync for the device and Unified CM database.

Explanation Configuration information may be out of sync for the device and Unified CM database

Recommended Action Go to Unified CM Administration and confirm that the device specified in this alarm actually exists in the database. If it does not, add the device. If the device is found in Unified CM Administration, examine the device information on the Device Configuration page for this device to make certain that important device information such as MAC address, device name, device pool configuration, and so on are configured accurately. If you find a discrepancy, correct it and reset the device.

Error Message

%UC_CALLMANAGER-3-DbInfoTimeout: %[DeviceName=String][AppID=String][ClusterID=String] [NodeID=String]: Unified CM did not receive a timely response from the database.

Explanation Unified CM requested information about the device specified in this alarm but the Unified CM Administration database did not respond before the internally-configured wait timer in Unified CM expired. Delays can occur because of congestion in accessing the database.

Recommended Action Go to the Cisco Unified Reporting web page, generate a Unified CM Database Status report and verify that the report shows that "Local and publisher databases are accessible" and that "all servers have a good replication status". If database status and DB replications look good, the database may be busy with auto-registrations or other intensive tasks. If you know that auto-registration is proceeding for a large number of devices, wait for it to complete (you can also monitor by watching the CPU level on the database server) and allow the phone to attempt to auto-register again.

Error Message

%UC_CALLMANAGER-3-DbInfoCorrupt: %[DeviceName=String][AppID=String][ClusterID=String] [NodeID=String]: Configuration information may be out of sync for the device and Unified CM database.

Explanation Configuration information may be out of sync for the device and Unified CM database

Recommended Action Go to Unified CM Administration and confirm that the device specified in this alarm actually exists in the database. If it does not, add the device. If the device is found in Unified CM Administration, examine the device information on the Device Configuration page for this device to make certain that important device information such as MAC address, device name, device pool configuration, and so on are configured accurately. If you find a discrepancy, correct it and reset the device.

Error Message

%UC_CALLMANAGER-4-NotEnoughChans: %[DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: Not enough channels.

Explanation A call attempt was rejected because the 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.

Recommended Action Add more gateway resources; Check the Cisco CallManager 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.

Error Message

%UC_CALLMANAGER-6-DeviceResetInitiated: %[{Optional}DeviceName=String][ProductType=String][{Optional}DeviceType=Enum][AppID=String][ClusterID=String][NodeID=String]: Device reset initiated on the specified device.

Explanation 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 Unified CM.

Recommended Action Informational purposes only; no action is required

Reason Code - Enum Definitions

Enum Definitions - DeviceType

Value	Definition
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
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
254	UNKNOWN_MGCP_GATEWAY
255	UNKNOWN
30027	ANALOG_PHONE
30028	ISDN_BRI_PHONE
30032	SCCP_GATEWAY_VIRTUAL_PHONE

Error Message

%UC_CALLMANAGER-6-EndPointResetInitiated: %[DeviceName=String][ProductType=String][DeviceType=Enum][AppID=String][ClusterID=String][NodeID=String]: Endpoint reset initiated on the specified endpoint.

Explanation 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 Unified CM.

Recommended Action Informational purposes only; no action is required

Reason Code - Enum Definitions

Enum Definitions - DeviceType

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
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
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

Error Message

%UC_CALLMANAGER-6-DeviceRestartInitiated: %[{Optional}DeviceName=String] [ProductType=String][{Optional}DeviceType=Enum][AppID=String][ClusterID=String] [NodeID=String]: Device restart initiated or Apply Config initiated on the specified device.

Explanation 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 re-register with Cisco Unified Communications Manager (Unified CM) without shutting down. A device can be restarted only when it is registered with Unified CM.

Recommended Action Informational purposes only; no action is required

Reason Code - Enum Definitions

Enum Definitions - DeviceType

Value	Definition
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
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
254	UNKNOWN_MGCP_GATEWAY
255	UNKNOWN
30027	ANALOG_PHONE
30028	ISDN_BRI_PHONE
30032	SCCP_GATEWAY_VIRTUAL_PHONE

Error Message

%UC_CALLMANAGER-6-EndPointRestartInitiated: %[DeviceName=String][ProductType=String][DeviceType=Enum][AppID=String][ClusterID=String][NodeID=String]: Endpoint restart initiated or Apply Config initiated on the specified endpoint.

Explanation This alarm occurs when an endpoint is restarted via the Restart button in Cisco Unified CM Administration window or when a system administrator presses the Apply Config button for an endpoint that does not support conditional restart. Restart causes the endpoint to unregister, receive an updated configuration file, and re-register with Cisco Unified Communications Manager (Unified CM) without shutting down. An endpoint can be restarted only when it is registered with Unified CM.

Recommended Action Informational purposes only; no action is required

Reason Code - Enum Definitions

Enum Definitions - DeviceType

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
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
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

Error Message

%UC_CALLMANAGER-6-DeviceApplyConfigInitiated: %[{Optional}DeviceName=String] [ProductType=String][{Optional}DeviceType=Enum][AppID=String][ClusterID=String] [NodeID=String]: An Apply Config action was initiated by a system administrator for the specified device.

Explanation 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.

Recommended Action Informational purposes only; no action is required

Reason Code - Enum Definitions

Enum Definitions - DeviceType

Value	Definition
493	CISCO_9971

Error Message

%UC_CALLMANAGER-4-DaTimeOut: %[AppID=String][ClusterID=String][NodeID=String]: The digit analysis component in Unified CM has timed out.

Explanation The digit analysis component in Unified CM has timed out. This can occur because Unified CM is busy and the resulting delay in processing request and response messages caused the digit analysis component to time out.

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 Unified CM.

Error Message

%UC_CALLMANAGER-5-MaxCallDurationTimeout: %[MaxCallDuration=UInt] [OriginatingDevice=String][DestinationDevice=String][CallStartTime=UInt][CallStopTime=UInt] [CallingPartyNumber=String][CalledPartyNumber=String][AppID=String][ClusterID=String] [NodeID=String]: Maximum call duration timer has expired.

Explanation An active call was cleared because the amount of time specified in the Maximum Call Duration Timer service parameter has 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.

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.

Error Message

%UC_CALLMANAGER-6-MaxHoldDurationTimeout: %[MaxHoldDuration=Int] [OriginatingDevice=String][DestinationDevice=String][HoldStartTime=UInt][HoldStopTime=UInt] [CallingPartyNumber=String][CalledPartyNumber=String][AppID=String][ClusterID=String] [NodeID=String]: Maximum Hold Duration Timer expired.

Explanation A held call was cleared because the amount of time specified in the Maximum Hold Duration Timer service parameter has 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.

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

Error Message

%UC_CALLMANAGER-2-TimerThreadSlowed: %[AppID=String][ClusterID=String] [NodeID=String]: Timer thread has slowed beyond acceptable limits.

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

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 the Cisco Technical Assistance Center (TAC)

Error Message

%UC_CALLMANAGER-6-DatabaseDefaultsRead: %[AppID=String][ClusterID=String] [NodeID=String]: Database default information was read successfully.

Explanation Database default information was read successfully; this alarm will be removed in Unified CM release 10.0(0).

Recommended Action Informational purposes only; no action is required

Error Message

%UC_CALLMANAGER-3-DeviceInitTimeout: %[DeviceName=String][Protocol=String][Side=UInt] [AppID=String][ClusterID=String][NodeID=String]: Device initialization timed out due to internal error.

Explanation A device initialization timeout occurred because the device did not respond to an initialize request. If this alarm occurs in tandem with a configuration change, this may not indicate a problem unless this alarm recurs.

Recommended Action If you are making a configuration change around the time that this alarm occurred, determine whether the problem still exists by calling the phone or placing a call through the trunk or gateway. If the call fails, reset the device. If the alarm recurs after resetting the device, review the System Reports provided in the Cisco Unified Reporting tool, specifically the Unified CM Database Status report, for any anomalous activity. 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. Check network connectivity to the server that is running the database.

Error Message

%UC_CALLMANAGER-3-NumDevRegExceeded: %[MaxDevices=Int][AppID=String][ClusterID=String] [NodeID=String]: The allowed number of registered devices has been exceeded.

Explanation The allowed number of registered devices, as controlled by the Cisco CallManager service parameter Maximum Number of Registered Devices, has been exceeded

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 it's 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.

Error Message

%UC_CALLMANAGER-5-CallManagerOnline: %[CCMVersion=String][AppID=String][ClusterID=String][NodeID=String]: Cisco CallManager service is online.

Explanation The Cisco CallManager service has completed initialization and is online

Recommended Action Informational purposes only; no action is required

Error Message

%UC_CALLMANAGER-4-OutOfRangeMohAudioSource: %[MohAudioSourceId=UInt][MaxMohAudioSourceId=UInt][AppID=String][ClusterID=String][NodeID=String]: Music On Hold Audio Source ID is invalid.

Explanation This alarm occurs when Music On Hold fails because the MOH audio source ID requested is not within the valid range of 1 - (Maximum value parameter in this alarm). The caller will hear Tone-on-Hold instead of the desired Music on Hold audio.

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 SIP Trunk Call then the value must be corrected at the source of this header. Otherwise, check the values for the MOH audio source in the Call Manager service parameter settings or possibly other configuration settings related to the party that initiated the hold.

Error Message

%UC_CALLMANAGER-4-UnprovisionedMohAudioSource: %[MohAudioSourceId=UInt][AppID=String][ClusterID=String][NodeID=String]: Music On Hold Audio Source ID is not provisioned.

Explanation This alarm occurs when Music On Hold fails because the MOH audio source ID 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.

Recommended Action Check the Music On Hold Audio Source list within CUCM Administration to ensure it has been assigned (provisioned) to an audio wav file or if ID# 51 is being used that the MOH Fixed Audio source has been enabled. Note that audio files must be uploaded using the CUCM Administration page of each MOH server in the cluster before that server can play the audio file.

Error Message

%UC_CALLMANAGER-4-BuiltInBridgeNoMoreResourcesAvailable: %[DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: BuiltInBridge resource allocation failed.

Explanation Built In Bridge resource allocation failed for one/more of the reasons --> 1)The device is not able to support built in conference 2)The built in resource of the device is already in use by another feature or application

Recommended Action Check to be sure that device involved in the call has the Built In Bridge resource and it is enabled. Consider install additional Built in Bridge resources

Error Message

%UC_CALLMANAGER-4-MtpNoMoreResourcesAvailable: %[MediaResourceListName=String][AppID=String][ClusterID=String][NodeID=String]: MTP or transcoder allocation failed.

Explanation 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 RFC 2833 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).

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 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. It's a good idea 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.

Error Message

%UC_CALLMANAGER-4-MohNoMoreResourcesAvailable: %[MediaResourceListName=String] [AppID=String][ClusterID=String][NodeID=String]: MOH resource allocation failed.

Explanation 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.

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, 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).

Error Message

%UC_CALLMANAGER-4-ConferenceNoMoreResourcesAvailable: %[MediaResourceListName=String] [AppID=String][ClusterID=String][NodeID=String]: Conference resource allocation failed.

Explanation 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

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.

Error Message

%UC_CALLMANAGER-4-AnnunciatorNoMoreResourcesAvailable: %[MediaResourceListName=String] [AppID=String][ClusterID=String][NodeID=String]: Annunciator resource allocation failed.

Explanation 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.

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 Media Resources > Annunciator 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. If the MTP or transcoder is not allocated, 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.

Error Message

%UC_CALLMANAGER-3-RsvpNoMoreResourcesAvailable: %[MediaResourceListName=String] [AppID=String][ClusterID=String][NodeID=String]: RSVP Agent resource allocation failed.

Explanation This 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 RFC 2833 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).

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 an upgraded version supports 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 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 only be done 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 in Cisco Unified CM Administration and click the appropriate Media Resource Group List, then 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 endpoint 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 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 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.

Error Message

%UC_CALLMANAGER-2-MaxCallsReached: %[Count=Int][AppID=String][ClusterID=String] [NodeID=String]: Maximum calls of simultaneous calls in this node has been reached.

Explanation The maximum number of simultaneous connections in a 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.

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.

Error Message

%UC_CALLMANAGER-1-DBLException: %[ErrorCode=Int][ExceptionString=String][AppID=String] [ClusterID=String][NodeID=String]: An error occurred while performing database activities.

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

Recommended Action Review the System Reports provided in the Cisco Unified Reporting tool, specifically the Unified CM Database Status report, for any anomalous activity. 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. Check network connectivity to the server that is running the database. If your system uses DNS, check the DNS configuration for any errors. If the cause is still not identified, collect SDL and SDI traces and contact the Cisco Technical Assistance Center (TAC).

Error Message

%UC_CALLMANAGER-3-ICTCallThrottlingStart: %[DeviceName=String][IPAddress=String] [{Optional}DeviceType=Enum][{Optional}Description=String][AppID=String][ClusterID=String] [NodeID=String]: Unified CM stops handling calls for the indicated H.323 device due to heavy traffic or a route loop over the H.323 trunk.

Explanation Unified CM 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.

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 the Cisco Technical Assistance Center (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.

Reason Code - Enum Definitions

Enum Definitions - DeviceType

Value	Definition
125	TRUNK

Error Message

%UC_CALLMANAGER-5-ICTCallThrottlingEnd: %[DeviceName=String][IPAddress=String] [{Optional}DeviceType=Enum][{Optional}Description=String][AppID=String][ClusterID=String] [NodeID=String]: Unified CM starts handling calls again for the indicated H.323 device.

Explanation Unified CM has ceased throttling calls on the indicated H.323 device

Recommended Action Notification purposes only; no action is required

Reason Code - Enum Definitions

Enum Definitions - DeviceType

Value	Definition
125	TRUNK

Error Message

%UC_CALLMANAGER-2-CodeYellowEntry: %[AverageDelay=UInt][EntryLatency=UInt] [ExitLatency=UInt][SampleSize=UInt][TotalCodeYellowEntry=UInt][HighPriorityQueueDepth=Long] [NormalPriorityQueueDepth=Long][LowPriorityQueueDepth=Long][AppID=String][ClusterID=String] [NodeID=String]: Unified CM has entered Code Yellow state.

Explanation Unified CM has initiated call throttling due to unacceptably high delay in handling incoming calls

Recommended Action Memory problems or high CPU usage are generally at the root of a Code Yellow condition. 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). Use RTMT to check for memory leaks, causes of any CPU spikes, and determine whether the server has sufficient memory for the tasks expected of this server. Run server diagnostics to determine if the disk is bad, and examine/reconfigure the SDL trace settings in Unified Serviceability to ensure that trace settings are not contributing to Code Yellow. You can determine the level of fragmentation on the hard disk by issuing the File Fragmentation command from the CLI for the trace directories. After taking one or more of these corrective actions, 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 triggering the CodeYellowEntry alarm, contact the Cisco Technical Assistance Center (TAC) and supply the trace information you have collected

Error Message

%UC_CALLMANAGER-5-CodeYellowExit: %[AverageDelay=UInt][EntryLatency=UInt] [ExitLatency=UInt][SampleSize=UInt][TimeSpentInCodeYellow=UInt] [NumberOfCallsRejectedDueToCallThrottling=UInt][TotalCodeYellowExit=UInt]

[HighPriorityQueueDepth=Long][NormalPriorityQueueDepth=Long][LowPriorityQueueDepth=Long] [AppID=String][ClusterID=String][NodeID=String]: Unified CM has exited Code Yellow.

Explanation Unified CM has ceased throttling calls and has exited the Code Yellow state

Recommended Action Notification purposes only; no action is required

Error Message

%UC_CALLMANAGER-2-CodeRedEntry: %[AverageDelay=UInt][EntryLatency=UInt][ExitLatency=UInt] [SampleSize=UInt][CodeYellowDuration=UInt][NumberOfCallsRejectedDueToCallThrottling=UInt] [TotalCodeYellowEntry=UInt][TotalCodeYellowExit=UInt][HighPriorityQueueDepth=Long] [NormalPriorityQueueDepth=Long][LowPriorityQueueDepth=Long][AppID=String][ClusterID=String] [NodeID=String]: Unified CM has entered Code Red condition and will restart.

Explanation 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.

Recommended Action Make certain that you 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 occurs automatically.

Error Message

%UC_CALLMANAGER-2-SignalCongestionEntry: %[Thread=String][AverageDelay=UInt] [EntryLatency=UInt][ExitLatency=UInt][SampleSize=UInt][TotalSignalCongestionEntry=UInt] [HighPriorityQueueDepth=Long][NormalPriorityQueueDepth=Long][LowPriorityQueueDepth=Long] [AppID=String][ClusterID=String][NodeID=String]: Unified CM has detected signal congestion in an internal thread and has throttled activities for that thread.

Explanation Unified CM has initiated throttling for an internal thread due to unacceptably high delay in handling signals

Recommended Action Memory problems or high CPU usage are generally at the root of signal congestion. 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). Use RTMT to check for memory leaks, causes of any CPU spikes, and determine whether the server has sufficient memory for the tasks expected of this server. Run server diagnostics to determine if the disk is bad, and examine/reconfigure the SDL trace settings in Unified Serviceability to ensure that trace settings are not contributing to the signal congestion. You can determine the level of fragmentation on the hard disk by issuing the File Fragmentation command from the CLI for the trace directories. After taking one or more of these corrective actions, monitor the situation and collect existing trace files. If the SignalCongestionExit alarm is not issued in a reasonable amount of time as deemed by your organization, or if the system is frequently triggering the SignalCongestionEntry alarm, contact the Cisco Technical Assistance Center (TAC) and supply the trace information you have collected.

Error Message

%UC_CALLMANAGER-5-SignalCongestionExit: %[Thread=String][AverageDelay=UInt] [EntryLatency=UInt][ExitLatency=UInt][SampleSize=UInt][TimeSpentInSignalCongestion=UInt] [NumberOfCallsRejected=UInt][TotalSignalCongestionExit=UInt][HighPriorityQueueDepth=Long]

[NormalPriorityQueueDepth=Long][LowPriorityQueueDepth=Long][AppID=String][ClusterID=String][NodeID=String]: Unified CM has exited throttling caused by a previous signal congestion condition.

Explanation Unified CM has exited the throttling state caused by signal congestion on a threaded process within Unified CM

Recommended Action Notification purposes only; no action is required

Error Message

%UC_CALLMANAGER-2-MemoryThrottlingEntry: %[ConfiguredVMSize=Int][ConfiguredFreeOrdBlocks=Int][ThrottledVMSize=Int][ThrottledFreeOrdBlocks=Int][AppID=String][ClusterID=String][NodeID=String]: Unified CM has entered a memory throttling state; new call attempts are being rejected.

Explanation Unified CM has initiated call throttling due to unacceptably high memory usage

Recommended Action High traffic usage is generally the root cause of a memory throttling condition. Evaluate the load balancing amongst the servers in your deployment to determine if additional nodes are needed to handle the traffic. If the MemoryThrottlingExit alarm is not issued in a reasonable amount of time as deemed by your organization, or if the system is frequently triggering the MemoryThrottlingEntry alarm, contact the Cisco Technical Assistance Center (TAC) for assistance

Error Message

%UC_CALLMANAGER-5-MemoryThrottlingExit: %[ConfiguredVMSize=Int][ConfiguredFreeOrdBlocks=Int][ThrottledVMSize=Int][ThrottledFreeOrdBlocks=Int][MemoryThrottlingExitReason=String][AppID=String][ClusterID=String][NodeID=String]: Unified CM has exited a memory throttling state.

Explanation Unified CM has ceased throttling calls and has exited the memory throttling state

Recommended Action Notification purposes only; no action is required

Error Message

%UC_CALLMANAGER-3-DeviceCloseMaxEventsExceeded: %[TotalEventsReceived=UInt][IPAddress=String][TCPHandle=String][MaxEventsAllowed=UInt][NumberOfSkinnyDeviceThrottled=UInt][AppID=String][ClusterID=String][NodeID=String]: 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.

Explanation 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.

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.

Error Message

%UC_CALLMANAGER-4-MaliciousCall: %[CalledPartyNumber=String][CalledDeviceName=String][CalledDisplayName=String][CallingPartyNumber=String][CallingDeviceName=String]

[CallingDisplayName=String][AppID=String][ClusterID=String][NodeID=String]: A malicious call has been identified.

Explanation A user presses the MCID softkey to alert you that the call indicated in this alarm contained disturbing content. This is not to indicate a voice quality issue on the call but to alert you to a potentially abusive or offensive occurrence involving the calling party device.

Recommended Action After a user presses the MCID softkey, the MCID service flags the call detail record (CDR) with the MCID notice and sends a notification to the PSTN that a malicious call is in progress. Take appropriate action as defined by your company policy regarding disturbing/abusive calls.

Error Message

%UC_CALLMANAGER-4-BeginThrottlingCallListBLFSubscriptions: %[ActiveExternalPresenceSubscriptions=UInt][CallListBLFSubscriptionsThrottlingThreshold=UInt][CallListBLFSubscriptionsResumeThreshold=UInt][TotalBeginThrottlingCallListBLFSubscriptions=UInt][AppID=String][ClusterID=String][NodeID=String]: Unified CM has initiated throttling of CallList BLF subscriptions as a preventive measure to avoid overloading the system.

Explanation Unified CM has initiated throttling of Call List BLF subscriptions as a preventive measure to avoid overloading the system. This alarm occurs when the total number of active BLF subscriptions exceeds the configured limit set by the Presence Subscription Throttling Threshold service parameter.

Recommended Action Determine if CPU and memory resources are available to meet the higher demand for CallList BLF subscriptions. If so, increase the value in the Cisco CallManager service parameter Presence Subscription Throttling Threshold and correspondingly reduce the value in the Presence Subscription Resume Threshold service parameter. If you do not have sufficient CPU and memory resources to increase the throttling threshold value, evaluate a plan to increase system resources to meet the demand.

Error Message

%UC_CALLMANAGER-5-EndThrottlingCallListBLFSubscriptions: %[ActiveExternalPresenceSubscriptions=UInt][CallListBLFSubscriptionsThrottlingThreshold=UInt][CallListBLFSubscriptionsResumeThreshold=UInt][TimeDurationOfThrottlingCallListBLFSubscriptions=UInt][NumberOfCallListBLFSubscriptionsRejectedDueToThrottling=UInt]

[TotalEndThrottlingCallListBLFSubscriptions=UInt][AppID=String][ClusterID=String] [NodeID=String]: EndThrottlingCallListBLFSubscriptions.

Explanation Unified CM has resumed accepting CallList BLF subscriptions subsequent to prior throttling

Recommended Action Notification purposes only; no action is required

Error Message

%UC_CALLMANAGER-5-PktCapServiceStarted: %[AppID=String][ClusterID=String] [NodeID=String]: Packet capture service has started.

Explanation The packet capture feature has been enabled on the Unified CM server. A Cisco CallManager service parameter, Packet Capture Enable, must be set to True for packet capture to occur.

Recommended Action Informational purposes only; no action is required

Error Message

%UC_CALLMANAGER-5-PktCapServiceStopped: %[AppID=String][ClusterID=String] [NodeID=String]: Packet capture service has stopped.

Explanation The packet capture feature has been disabled in Unified CM

Recommended Action Informational purposes only; no action is required

Error Message

%UC_CALLMANAGER-5-PktCapOnDeviceStarted: %[DeviceName=String][Mode=String] [Duration=String][AppID=String][ClusterID=String][NodeID=String]: Packet capture has started on the device.

Explanation Packet capture has been enabled on the device indicated in this alarm

Recommended Action Informational purposes only; no action is required

Error Message

%UC_CALLMANAGER-5-PktCapOnDeviceStopped: %[DeviceName=String][Mode=String] [Duration=String][AppID=String][ClusterID=String][NodeID=String]: Packet capture stopped on the device.

Explanation Packet capture has been disabled on the indicated device

Recommended Action Informational purposes only; no action is required

Error Message

%UC_CALLMANAGER-4-UserUserPrecedenceAlarm: %[DeviceName=String][Reason=Enum] [AppID=String][ClusterID=String][NodeID=String]: User-to-User Precedence passing violation.

Explanation User-to-User IE was not successfully tunneled to destination; please refer to reason code for additional details

Recommended Action Refer to the information (help text) in the reason code in this alarm for detailed actions

Reason Code - Enum Definitions

Enum Definitions - Reason

Value	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 IE ID 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).

Error Message

%UC_CALLMANAGER-3-MultipleSIPTrunksToSamePeerAndLocalPort: %[PeerIPAddr=String] [LocalIPport=UInt][oldDeviceName=String][oldDeviceInstance=String][newDeviceName=String] [newDeviceInstance=String][AppID=String][ClusterID=String][NodeID=String]: A conflict occurred because multiple trunks have been configured to the same destination and local port.

Explanation 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 new trunk invalidated the old trunk.

Recommended Action Check the SIP Trunk Configuration in Cisco Unified CM Administration and ensure that only one SIP trunk is configured to the same destination address and local port

Error Message

%UC_CALLMANAGER-0-NoFeatureLicense: %[AppID=String][ClusterID=String][NodeID=String]: No feature license found.

Explanation 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).

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)

Error Message

%UC_CALLMANAGER-6-CMInitializationStateTime: %[InitializationState=String] [CurrentStateTime=String][CurrentStateTimeMs=UInt][AppID=String][ClusterID=String]

[NodeID=String]: Indicates the amount of time it took for Unified CM to initialize each state in the initialization process.

Explanation Indicates the amount of time required to complete initialization for the specified state

Recommended Action Informational purposes only; no action is required

Error Message

%UC_CALLMANAGER-6-CMTotalInitializationStateTime: %[TotalInitializationTime=String] [TotalInitializationTimeMs=UInt][AppID=String][ClusterID=String][NodeID=String]: Total amount of time it took for Unified CM to complete initialization.

Explanation Indicates the amount of time required to complete the total system initialization

Recommended Action Informational purposes only; no action is required

Error Message

%UC_CALLMANAGER-1-CMOverallInitTimeExceeded: %[CMOverallInitializationTime=Int] [AppID=String][ClusterID=String][NodeID=String]: Initialization of the Unified CM system has taken longer than allowed by the System Initialization Timer service parameter; the system automatically restarts to attempt initialization again.

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

Recommended Action 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).

Error Message

%UC_CALLMANAGER-4-DigitAnalysisTimeoutAwaitingResponse: %[TranslationPatternTriggeringPoint=String][PolicyDecisionPoint=String][AppID=String] [ClusterID=String][NodeID=String]: Unified CM sent a routing request to the policy decision point but the request timed out without a response.

Explanation Unified CM was unable to complete the routing request before timing out. This timeout 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.

Recommended Action Check the External Call Control object in Real-Time Monitoring Tool (RTMT) to see whether the ExternalCallControlEnabledCallAttempted counter is spiking. A dramatic increase in that counter indicates an unusually high number of calls at this time which could result in reduced system resources. Check the QueueSignalsPresent2-Normal counter 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).

Error Message

%UC_CALLMANAGER-3-InvalidIPNetPattern: %[Description=String][IPAddress=String] [DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: An invalid IP address is configured in one or more SIP route patterns in Cisco Unified CM Administration.

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

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.

Error Message

%UC_CALLMANAGER-4-FailedToFulfillDirectiveFromPDP: %[PolicyDecisionPoint=String] [FailedToFulfillReason=String][CalledPartyNumber=String][CallingPartyNumber=String] [CallingUserId=String][AppID=String][ClusterID=String][NodeID=String]: Unified CM cannot fulfill the call routing directive returned by the policy decision point.

Explanation A routing directive from the policy decision point (PDP) cannot be fulfilled. This could occur because the call was cleared by a CTI application before Unified CM was able to route it to the location defined by the PDP; because a call that was allowed by a policy server was redirected by the CTI application to a destination; because the annunciator ID was misconfigured in the PDP; or because Unified CM attempted to invoke a media resource such as Annunciator but no resources were available.

Recommended Action In many cases, a failure to fulfill a routing directive occurs because of intervention by a CTI application which scoops up the call before Unified CM is able to fulfill the routing directive in the PDP. If CTI interaction is having a negative effect, examine the CTI application to ensure that the call is in alerting or connected state before CTI begins to interact with the call. If the failure is caused by a problem with the annunciator ID, check to be sure 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.

Error Message

%UC_CALLMANAGER-3-FailureResponseFromPDP: %[PolicyDecisionPoint=String] [StatusCodeAndReasonPhrase=String][AppID=String][ClusterID=String][NodeID=String]: The policy decision point returned a 4xx (client) or 5xx (server) status code in the HTTP response.

Explanation 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 RFC 2616 for detailed explanations about HTTP Status Code definitions.

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 external call control profiles and external call control 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 external call control 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.

Error Message

%UC_CALLMANAGER-3-ConnectionFailureToPDP: %[PolicyDecisionPoint=String][FailedToConnectReason=String][AppID=String][ClusterID=String][NodeID=String]: A connection request from Unified CM to the policy decision point failed.

Explanation A connection request to the policy decision point (PDP) failed. Failure may have been due to a network error causing limited or no connectivity between Unified CM and the PDP; because of authentication errors when Unified CM established an HTTPS connection to the PDP; or because the PDP was not in service.

Recommended Action Verify that network connectivity exists 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, make sure that the PDP service is active.

Error Message

%UC_CALLMANAGER-6-ConnectionToPDPInService: %[PolicyDecisionPoint=String][AppID=String][ClusterID=String][NodeID=String]: A connection was successfully established between Unified CM and the policy decision point.

Explanation A successful connection from Unified CM to the policy decision point (PDP) has been established

Recommended Action Informational purposes only; no action is required

Error Message

%UC_CALLMANAGER-3-AwaitingResponseFromPDPTimeout: %[PolicyDecisionPoint=String][AppID=String][ClusterID=String][NodeID=String]: Unified CM timed out waiting for the routing response from the policy decision point.

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

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: 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 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.

Error Message

%UC_CALLMANAGER-3-ErrorParsingDirectiveFromPDP: %[PolicyDecisionPoint=String] [CalledPartyNumber=String][CallingPartyNumber=String][CallingUserId=String] [ResponseXMLData=String][AppID=String][ClusterID=String][NodeID=String]: Unified CM failed to parse the call routing directive or the diversion destination in the call routing response from the policy decision point.

Explanation A routing response was received but 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.

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.

Error Message

%UC_CALLMANAGER-4-ErrorParsingResponseFromPDP: %[PolicyDecisionPoint=String] [CalledPartyNumber=String][CallingPartyNumber=String][CallingUserId=String] [RequestXMLData=String][AppID=String][ClusterID=String][NodeID=String]: Unified CM failed to parse one or multiple optional elements or attributes in the call routing response from the policy decision point.

Explanation A routing response was received from the policy decision point (PDP) but 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.

Recommended Action Confirm that the call routing response from the policy decision point complies with the guidelines specified for external call control in the Cisco Unified Communications Manager documentation. Confirm that 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.

Error Message

%UC_CALLMANAGER-4-CallAttemptBlockedByPolicy: %[PolicyDecisionPoint=String] [RejectReason=String][CalledPartyNumber=String][CallingPartyNumber=String][CallingUserId=String] [AppID=String][ClusterID=String][NodeID=String]: A call was attempted but blocked or rejected by the policy decision point.

Explanation A call was rejected or blocked because it violated the enterprise policy as defined in a policy decision point (PDP) that was configured in 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.

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.

Error Message

%UC_CALLMANAGER-5-ServicePortOnline: %[Protocol=String][PortNumber=UInt][AppID=String] [ClusterID=String][NodeID=String]: A Cisco CallManager service port is online.

Explanation Unified CM has successfully opened a socket port to provide service

Recommended Action Notification purposes only; no action is required

Error Message

%UC_CALLMANAGER-2-ServicePortOffline: %[Protocol=String][PortNumber=UInt][ErrorNumber=Int] [AppID=String][ClusterID=String][NodeID=String]: A Unified CM service port is offline.

Explanation A Unified CM socket port that is used to provide service has unexpectedly closed; Unified CM will attempt to reopen this port. Normally, this port should never be closed. An unexpected closing of this port generally indicates an operating system failure or an external attack on Unified CM.

Recommended Action Verify that Unified CM is able to reopen this socket port and provide service. You can watch for an instance of the notice level alarm, ServicePortOnline, when service to the port has been restored. If the port is not reopened and service restored, restart the Cisco CallManager service. If this alarm occurs for an extended duration, collect the existing trace files and contact the Cisco Technical Assistance Center (TAC).

Error Message

%UC_CALLMANAGER-4-SuspiciousIPAddress: %[PortNumber=UInt][Address=String][AppID=String] [ClusterID=String][NodeID=String]: Unified CM has identified suspicious connection attempts from an IP address.

Explanation Unified CM has identified suspicious connection attempts from an IP address and has temporarily blocked the address. This alarm is an indication that a Denial-of-Service attack may have been attempted from this IP address.

Recommended Action Examine network activity for repeated attempts to access the port number specified in this alarm. Using the IP address specified in this alarm, attempt to identify the device that has been sending connection attempts to the port. If the IP address belongs to a device that is configured in Unified CM, evaluate the possible reason for such numerous connection attempts. Generally, no device that is functioning properly will trigger this alarm. Reset the device or remove the device from the network.

Error Message

%UC_CALLMANAGER-3-LostConnectionToSAFForwarder: %[IPAddress=String] [SafClientHandle=UInt][AppID=String][ClusterID=String][NodeID=String]: Connection to the SAF Forwarder has been lost.

Explanation 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.

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.

Error Message

%UC_CALLMANAGER-3-SAFForwarderError: %[IPAddress=String][SafClientHandle=UInt] [ApplicationUserName=String][ReasonCode=Enum][SAFProtocolVersion=String][ServiceID=UInt] [SubServiceID=UInt][AppID=String][ClusterID=String][NodeID=String]: SAF Forwarder error response sent to Unified CM.

Explanation Unified CM received an error from the SAF Forwarder

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

Reason Code - Enum Definitions

Enum Definitions - ReasonCode

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).
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.
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 alarmfor 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")

Error Message

%UC_CALLMANAGER-6-SAFUnknownService: %[ClientHandle=String][ServiceID=UInt] [SubServiceID=UInt][InstanceID1=UInt][InstanceID2=UInt][InstanceID3=UInt][InstanceID4=UInt] [AppID=String][ClusterID=String][NodeID=String]: Unified CM does not recognize the service ID in a Publish Revoke or Withdraw message.

Explanation 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.

Recommended Action This alarm is for informational purposes only; no action is required

Error Message

%UC_CALLMANAGER-6-SAFPublishRevoke: %[ClientHandle=String][ServiceID=UInt] [SubServiceID=UInt][InstanceID1=UInt][InstanceID2=UInt][InstanceID3=UInt][InstanceID4=UInt] [AppID=String][ClusterID=String][NodeID=String]: A CLI command revoked the publish action for the specified service or subservice ID.

Explanation 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

Recommended Action Informational purposes only; no action is required

Error Message

%UC_CALLMANAGER-3-SAFResponderError: %[ClientHandle=String][ServiceID=UInt] [SubServiceID=UInt][InstanceID1=UInt][InstanceID2=UInt][InstanceID3=UInt][InstanceID4=UInt] [AppID=String][ClusterID=String][NodeID=String]: SAF Responder Error 500.

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

Recommended Action No action is required

Error Message

%UC_CALLMANAGER-3-DuplicateLearnedPattern: %[ClientHandle=String][ServiceID=UInt] [SubServiceID=UInt][InstanceID1=UInt][InstanceID2=UInt][InstanceID3=UInt][InstanceID4=UInt] [AppID=String][ClusterID=String][NodeID=String]: CCD requesting service received a duplicate Hosted DN.

Explanation 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.

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).

Error Message

%UC_CALLMANAGER-3-CCDIPReachableTimeOut: %[AppID=String][ClusterID=String] [NodeID=String]: CCD Requesting Service IP Reachable Duration Time Out.

Explanation 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.

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

Error Message

%UC_CALLMANAGER-3-CCDPSTNFailOverDurationTimeOut: %[AppID=String][ClusterID=String] [NodeID=String]: The internal limit on PSTN failover has expired.

Explanation 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.

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.

Error Message

%UC_CALLMANAGER-4-CCDLearnedPatternLimitReached: %[CCDMaxLearnedPatterns=UInt] [SystemLimitCCDLearnedPatterns=UInt][AppID=String][ClusterID=String][NodeID=String]: CCD has reached the maximum number of learned patterns allowed.

Explanation 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 inidcates that the CCD requesting service has met the maximum number of learned patterns allowed.

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.

Error Message

%UC_CALLMANAGER-5-DbInsertValidatedDIDFailure: %[e164DID=String][grantingDomain=String] [AppID=String][ClusterID=String][NodeID=String]: The Insertion of an IME-provided E.164 DID has failed.

Explanation A failure occurred attempting to insert a Cisco Unified Active Link learned DID

Recommended Action Verify the DID and the granting domain. Check other associated alarms. Verify the database integrity.

Error Message

%UC_CALLMANAGER-2-TCPSetupToIMEFailed: %[ip=String][port=UInt][AppID=String][ClusterID=String][NodeID=String]: Connection Failure to IME server.

Explanation 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.

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 Unified CM servers and the IME server.

Error Message

%UC_CALLMANAGER-1-TLSConnectionToIMEFailed: %[SSLErrorCode=UInt][SSLErrorText=String][AppID=String][ClusterID=String][NodeID=String]: TLS Failure to IME service.

Explanation 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).

Recommended Action Check to see that the certificate of the IME server is configured properly in the UCM.

Error Message

%UC_CALLMANAGER-1-InvalidCredentials: %[usr=String][ip=String][Server=String][AppID=String][ClusterID=String][NodeID=String]: Credential Failure to IME server.

Explanation 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

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.

Error Message

%UC_CALLMANAGER-1-IMEOverQuota: %[Server=String][Current quota=UInt][Maximum target quota=UInt][AppID=String][ClusterID=String][NodeID=String]: IME over quota.

Explanation 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, across all of the Unified CM clusters which are utilizing the same IME server, the quota for the IME distributed cache has been exceeded.

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. 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.

Error Message

%UC_CALLMANAGER-3-PublishFailedOverQuota: %[DID=String][Server=String][Current quota=UInt][Maximum target quota=UInt][AppID=String][ClusterID=String][NodeID=String]: Publish Failed - over Quota.

Explanation 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.

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.

Error Message

%UC_CALLMANAGER-4-PublishFailed: %[DID=String][AppID=String][ClusterID=String][NodeID=String]: Publish Failed.

Explanation 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.

Recommended Action If you notice single small numbers of this alarm 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.

Error Message

%UC_CALLMANAGER-3-IMEDistributedCacheInactive: %[AppID=String][ClusterID=String][NodeID=String]: Inactive IME distributed cache .

Explanation This alarm is generated when Unified CM attempts to connect to the IME server, however, the IME distributed cache is not currently active

Recommended Action Check to make sure that the IME certificate is provisioned on the IME server. Check to make sure that the IME distributed cache has been activated via the CLI on the IME server.

Error Message

%UC_CALLMANAGER-4-RejectedRoutes: %[Domain=String][DN=String][AppID=String][ClusterID=String][NodeID=String]: Rejected route due to Untrusted status.

Explanation This alarm is generated when Unified CM learned a route from the IME server. However, due to the configured Trusted/Untrusted list, the route was rejected.

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/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.

Error Message

%UC_CALLMANAGER-6-PublicationRunCompleted: %[StartTime=String][EndTime=String] [DIDCount=UInt][FailedDIDCount=UInt][FailedDIDs=String][AppID=String][ClusterID=String] [NodeID=String]: Completion of publication of published DID patterns.

Explanation This alarm is generated when Unified CM completes a publication of the DID patterns into the Cisco Intercompany Media Network

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 Cisco Intercompany Media 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.

Error Message

%UC_CALLMANAGER-6-RouteRemoved: %[RouteNumber=String][Domain=String] [RouteLearnedTime=String][Reason=Enum][AppID=String][ClusterID=String][NodeID=String]: Route removed automatically.

Explanation This alarm is generated when Unified CM removes a route from Unified CM Administration because the route is stale and has expired, or because the far end has indicated the number is no longer reachable at that domain

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.

Reason Code - Enum Definitions

Enum Definitions - Reason

Value	Definition
1	Expired
2	Unreachable

Error Message

%UC_CALLMANAGER-3-InsufficientFallbackIdentifiers: %[Profile=String][FallbackDN=String] [AppID=String][ClusterID=String][NodeID=String]: Cannot allocate fallback identifier.

Explanation 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.

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 in Cisco Unified CM Administration 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.

Error Message

%UC_CALLMANAGER-3-IMEQualityAlertEntry: %[ActiveCallCount=UInt][FallbackCallCount=UInt] [SetupAttempts=UInt][FailedAttempts=UInt][AppID=String][ClusterID=String][NodeID=String]: IME call quality problem.

Explanation This alarm is generated when Unified CM is seeing a substantial number of IME calls fail back to PSTN, or fail to be set up, due to IP network quality problems. There are two triggers for this alarm. One is when a large fraction of the currently active IME calls have all requested fallback, or have fallen back, to the PSTN. The other is when a large fraction of the recent call attempts have not been made over IP, and instead have gone to the PSTN.

Recommended Action Check your IP connectivity, and make sure it is good. If it looks good in general, you may need to look at CDRs, CMRs, and logs from the firewalls to determine what happened.

Error Message

%UC_CALLMANAGER-5-IMEQualityAlertExit: %[ActiveCallCount=UInt][FallbackCallCount=UInt] [SetupAttempts=UInt][FailedAttempts=UInt][AppID=String][ClusterID=String][NodeID=String]: IME call quality problem cleared.

Explanation This alarm is generated when the Unified CM sees a significant reduction in the number of failed IME calls following generation of the IMEQualityAlertEntry alarm. This notice alarm indicates that the IP connectivity issues causing the initial generation of the IMEQualityAlertEntry alarm have abated.

Recommended Action Continue to monitor IP connectivity for recurring issues

Error Message

%UC_CALLMANAGER-4-InvalidSubscription: %[SubscriptionId=UInt][IMEServer=String] [AppID=String][ClusterID=String][NodeID=String]: A message has been received from an IME server that contains a subscription identifier that is not handled by this node.

Explanation 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.

Recommended Action This may be a race condition if a 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.

Error Message

%UC_CALLMANAGER-3-FirewallMappingFailure: %[ip=String][port=UInt][AppID=String] [ClusterID=String][NodeID=String]: Firewall unreachable.

Explanation 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.

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.

Error Message

%UC_CALLMANAGER-3-ConflictingDataIE: %[DeviceName=String][AppID=String][ClusterID=String] [NodeID=String]: A call has been rejected because the incoming PRI/BRI Setup message had an invalid IE.

Explanation 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.

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

Error Message

%UC_CALLMANAGER-6-CalledPartyTracing: %[AppID=String][ClusterID=String] [NodeID=String]: Called Party Tracing Match found..

Explanation A call attempt has been made to a called party number being traced. Please check the Called Party Tracing log.

Recommended Action Use the Real Time Monitoring Tool to check the Called Party Tracing log.

Error Message

%UC_CALLMANAGER-4-SIP IPPortConflict: %[DeviceName=String][PortNumber=String] [{Optional}DeviceType=Enum][AppID=String][ClusterID=String][NodeID=String]: The local port for this device is already in use.

Explanation The local port specified for this device is already in use, or Cisco Unified CM Communications Manager is unable to bind to the configured port. Either the SIP device is configured incorrectly or the domain name system (DNS) is incorrectly configured.

Recommended Action In Cisco Unified CM Administration, check the port number for the SIP device.

Reason Code - Enum Definitions

Enum Definitions - DeviceType

Value	Definition
131	SIP_TRUNK

Error Message

%UC_CALLMANAGER-6-ConferenceCreated: %[ConferenceName=String][ConferenceID=UInt][VideoEnabled=UInt][ApplicationID=UInt][NumberOfStreams=UInt][Status=Int][Reason=Int][AppID=String][ClusterID=String][NodeID=String]: An application controlled conference is created..

Explanation An application controlled conference is created.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-6-ConferenceDeleted: %[ConferenceName=String][ConferenceID=UInt][Reason=Int][AppID=String][ClusterID=String][NodeID=String]: An application controlled conference is deleted..

Explanation An application controlled conference is deleted.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-4-CtiCallAcceptTimeout: %[CallAcceptTimer=UInt][DeviceName=String][CallingPartyDn=String][CalledPartyDn=String][AppID=String][ClusterID=String][NodeID=String]: Call Accept Timeout.

Explanation The application failed to accept the call within the CallAcceptTimer time period.

Recommended Action Configure the CallAcceptTimer service parameter appropriately based on the expected response time of the application.

Error Message

%UC_CALLMANAGER-6-CtiStaleCallHandle: %[Text=String][AppID=String][ClusterID=String][NodeID=String]: CTI stale call handle..

Explanation This alarm is issued by audit when it finds invalid call handles that the CTI application didn't close when calls go to idle state.

Recommended Action No action is required. It is recommended that the CTI applications explicitly close the calls when the call goes to idle state.

Error Message

%UC_CALLMANAGER-6-DatabaseAuditInfo_074: %[Number=Int][AppID=String][ClusterID=String][NodeID=String]: Database audit information..

Explanation Database audit information error occurred.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-5-DatabaseDeviceNoDirNum: %[Text=String][AppID=String][ClusterID=String][NodeID=String]: No directory number for database device..

Explanation No directory number(s) are associated with identified device.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-1-DatabaseInternalDataError_06e: %[DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: Database internal data error..

Explanation Database internal data error occurred.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-5-DatabaseInternalDataError_06f: %[RouteGroupName=String][AppID=String][ClusterID=String][NodeID=String]: Database internal data error..

Explanation Database internal data error occurred.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-6-DatabaseInternalDataError_070: %[DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: Database internal data error..

Explanation Database internal data error occurred.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-6-DatabaseInternalDataError_071: %[DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: Database internal data error..

Explanation Database internal data error occurred.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-6-DatabaseInternalDataError_072: %[DeviceName=String][AppID=String][ClusterID=String][NodeID=String]: Database internal data error..

Explanation Database internal data error occurred.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-6-DatabaseInternalDataError_073: %[DeviceType=String][AppID=String]

[ClusterID=String][NodeID=String]: Database internal data error..

Explanation Database internal data error occurred.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-6-DatabaseInternalDataError_075: %[Text=String][AppID=String] [ClusterID=String][NodeID=String]: Database internal data error..

Explanation Database internal data error occurred.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-3-DnTimeout: %[IsoEthPort=UInt][DSL=UInt][AppID=String][ClusterID=String] [NodeID=String]: DN Timeout..

Explanation Timeout was encountered while trying to read pattern or directory number configuration.

Recommended Action Investigate configuration for identified device.

Error Message

%UC_CALLMANAGER-4-H323AddressResolutionError: %[DeviceName=String][AppID=String] [ClusterID=String][NodeID=String]: H323 address not resolved..

Explanation An H323 device address could not be resolved. Cisco CallManager cannot handle calls to/from the indicated H323 device.

Recommended Action Either the H323 device entry is configured incorrectly, or the domain name system (DNS) is incorrectly configured.

Error Message

%UC_CALLMANAGER-4-H323CallFailureAlarm: %[PeerIPaddress=String][PeerIPport=UInt] [Reason=Enum][AppID=String][ClusterID=String][NodeID=String]: H323 Call failure.

Explanation H.323 inbound call fails because information required to route the call, including the source E.164 address, call signaling address, or H.323 ID, is missing.

Recommended Action No action needed.

Reason Code - Enum Definitions

Enum Definitions - Reason

Value	Definition
1	Unknown
2	SourceE164AddressNotFound
3	CallSignallingAddressNotFound
4	H323IdNotFound
5	SourceE164AddressOrCallSignallingAddressNotFound

Error Message

%UC_CALLMANAGER-4-MWIParamMisMatch: %[AppID=String][ClusterID=String] [NodeID=String]: MWI parameter mismatch..

Explanation Message waiting indicator number configuration error occurred.

Recommended Action Investigate message waiting indicator configuration.

Error Message

%UC_CALLMANAGER-4-OutOfDnForAutoRegistration: %[AppID=String][ClusterID=String] [NodeID=String]: Out of directory numbers for auto-registration..

Explanation Cisco CallManager ran out of directory numbers for auto-registration.

Recommended Action Investigate auto-registration configuration.

Error Message

%UC_CALLMANAGER-6-PktCapDownloadOK: %[File=String][AppID=String][ClusterID=String] [NodeID=String]: Downloaded captured packet or key file..

Explanation Indicated the packet or key file has been downloaded.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-3-PktCapDownloadFailed: %[File=String][FailedReason=String][AppID=String] [ClusterID=String][NodeID=String]: Did not get captured packet or key file..

Explanation Indicated reasons for the packet or key file could not be downloaded.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-6-PktCapLoginOK: %[UserID=String][AppID=String][ClusterID=String] [NodeID=String]: Login OK for getting captured packet or key file..

Explanation Indicated the user can get the packet or key file.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-3-PktCapLoginFailed: %[UserID=String][FailedReson=String][AppID=String] [ClusterID=String][NodeID=String]: Login failed for getting captured packet or key file..

Explanation Indicated the user cannot get the packet or key file.

Recommended Action It is required that the user is an valid End User under the user group called Standard Packet Sniffer Users.

Error Message

%UC_CALLMANAGER-3-ThrottlingSampleActivity: %[ThrottlingSampleActivity=Int][AppID=String] [ClusterID=String][NodeID=String]: ThrottlingSampleActivity.

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

Recommended Action Determine the reason for high CPU usage in the High priority and Normal priority queues (Cisco CallManager System Performance object).

Error Message

%UC_CALLMANAGER-6-GatewayAlarm: %[DeviceName=String][TCPHandle=VoidPtr] [DeviceText=String][Param1=UInt][Param2=UInt][AppID=String][ClusterID=String] [NodeID=String]: Gateway alarm..

Explanation Gateway device sent an alarm to Cisco CallManager.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-6-NoConnection: %[AppID=String][ClusterID=String][NodeID=String]: No TCP connection..

Explanation Disconnect or release request attempt occurred on unknown TCP connection.

Recommended Action No action is required.

Error Message

%UC_CALLMANAGER-6-TotalCodeYellowEntry: %[TotalCodeYellowEntry=Int][AppID=String] [ClusterID=String][NodeID=String]: TotalCodeYellowEntry.

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

Recommended Action Determine the reason for high CPU usage in the High priority and Normal priority queues (Cisco CallManager System Performance object).

Error Message

%UC_CALLMANAGER-5-DestinationCodeControlCallBlocked: %[RoutePattern=String] [BlockedCallPercentage=UInt][CallsAttempted=UInt][CallsRejected=UInt][AppID=String] [ClusterID=String][NodeID=String]: Call blocked by the Destination Code Control feature. .

Explanation Cisco Unified Communications Manager generates this alarm when a Destination Code Control feature enabled Route Pattern blocks a call.The route pattern blocks a call when it comes in at a time when the number of call attempts has reached the percentage of calls set to be blocked on this route pattern.

Recommended Action This alarm is provided for historic and informational purposes. It helps understand why certain calls through the DCC feature enabled route patterns are rejected. This historical information is useful to help determine how many calls to a particular route pattern were attempted and how many out of them were blocked. This data would help the administrator verify whether the percentage of Calls Blocked by the DCC feature is as per the configured percentage.

Error Message

%UC_CALLMANAGER-4-Redirection: %[ErrorMessage=String][AppID=String][ClusterID=String] [NodeID=String]: Redirection Manager cannot register with the Call Control..

Explanation The registration error occurs either when it registers itself or the REDIRECTION_OPERATIONIE_ID with the Call Control.

Recommended Action It is a code bug. No Action is Required.

Error Message

%UC_CALLMANAGER-3-CorruptedIncomingDMPropagationMessage: % [CorruptedRegElementsCount=UInt][CorruptedUnRegElementsCount=UInt][RemoteNodeID=UInt]

[AppID=String][ClusterID=String][NodeID=String]: Unified CM received a corrupted DMRemoteDeviceRegisterUnRegister message in internode communication.

Explanation Unified CM examines the incoming DMRemoteDeviceRegisterUnRegister messages to detect values in the message that are outside the normal expected range. Unified CM issues this alarm when the message is determined by Unified CM to contain values outside the normal range. Unified CM has discarded part of the contents of the incoming DMRemoteDeviceRegisterUnRegsister message due to the values that were out of range. This may cause an out-of-synch condition for the registered device's information between the sending node and this node, which in turn can lead to phone calls being routed incorrectly

Recommended Action Make a note of the IP address/name of the remote CM node that generated this message. Around the timestamp of this alarm, save the SDL/SDI logs from this node and the remote node for analysis by Cisco TAC personnel. Next, at the first opportunity, restart the Cisco CallManager service on this node to ensure that the registered devices information throughout the cluster are in synch. Also, in Cisco Unified Serviceability, make sure to set the Unified CM SDI logs setting to Detailed to ensure collecting relevant logs should this alarm recur. If this alarm does occur again, contact Cisco TAC to help determine the source of DMRemoteDeviceRegisterUnRegister message corruption.

Error Message

%UC_CALLMANAGER-6-UnEncryptedCallBlocked: %[Party1_CI=UInt][Party2_CI=UInt] [CallingPartyNumber=String][CalledPartyNumber=String][AppID=String][ClusterID=String] [NodeID=String]: Unencrypted call is blocked because one or both of the parties are non-secure or does not support compatible encryption capabilities and the service parameter BlockUnencryptedCalls is set to true..

Explanation Unencrypted call is blocked because one or both of the parties are non-secure or does not support compatible encryption capabilities and the service parameter BlockUnencryptedCalls is set to true.

Recommended Action Informational purposes only; no action is required

Error Message

%UC_CALLMANAGER-3-RecordingGatewayRegistrationRejected: %[GatewayAddress=String] [Cause=String][AppID=String][ClusterID=String][NodeID=String]: Registration to recording-enabled gateway rejected after multiple attempts; gateway marked out-of-service..

Explanation gateway rejected registration request

Recommended Action Cause value indicates reason registration was rejected. Check gateway web service api configuration. After configuration issue is resolved, reset SIP Trunk to attempt registration.

Error Message

%UC_CALLMANAGER-3-RecordingGatewayRegistrationTimeout: %[GatewayAddress=String] [Cause=String][AppID=String][ClusterID=String][NodeID=String]: No response from recording-enabled gateway after multiple attempts; timeout occurred; gateway marked out-of-service.

Explanation Gateway registration request did not complete within the specified time limit

Recommended Action Verify network connectivity between CUCM and gateway. Check IP address configuration. After configuration issue is resolved, reset SIP Trunk to attempt registration

Error Message

%UC_CALLMANAGER-5-RecordingGatewayOutOfService: %[GatewayAddress=String][Cause=String] [AppID=String][ClusterID=String][NodeID=String]: Recording-enabled gateway closed connection to

Unified CM .

Explanation Gateway status changed from in-service to out-of-service

Recommended Action Verify network connectivity between CUCM and gateway. Check IP address configuration. After configuration issue is resolved, reset SIP Trunk to attempt registration

Error Message

%UC_CALLMANAGER-5-RecordingGatewayInService: %[GatewayAddress=String][AppID=String] [ClusterID=String][NodeID=String]: Recording gateway status changed from out-of-service to in-service.

Explanation Gateway status changed from out-of-service to in-service

Recommended Action None

Error Message

%UC_CALLMANAGER-5-RecordingGatewaySessionFailed: %[GatewayAddress=String][Cause=String] [GatewayGuid=String][AppID=String][ClusterID=String][NodeID=String]: Gateway recording session terminated unexpectedly.

Explanation Cause value indicates reason the recording session terminated unexpectedly

Recommended Action Check gateway status

Error Message

%UC_CALLMANAGER-3-RecordingCallSetupFail: %[RecordedDeviceName=String] [RecordedDeviceDN=String][RecordingMediaPreference=Enum][RecordingMediaSource=Enum] [RecordingClusterID=String][RecordedDeviceCallID=UInt][GatewayGuid=String][CauseValue=UInt] [Reason=Enum][AppID=String][ClusterID=String][NodeID=String]: Recording call setup failed. There will be no recording.

Explanation Recording session setup failed

Recommended Action Determine which recording media resources are eligible to record the call based on the call flow (Phone, Gateway, or Both). Verify configuration of all eligible recording media resource (Phone, Gateway, or Both). If Cluster ID is displayed under AlarmValue, check SIP trunk configuration and gateway registration on other cluster.

Reason Code - Enum Definitions

Enum Definitions - RecordingMediaPreference

Value	Definition
1	Gateway Preferred
2	Phone Preferred
3	Phone Only

Enum Definitions - RecordingMediaSource

Value	Definition
1	Phone
2	Gateway

Enum Definitions - Reason

Value	Definition
1	Recording call setup failed
2	Recording request to other cluster timed out

Error Message

%UC_CALLMANAGER-4-RecordingResourcesNotAvailable: %[RecordedDeviceName=String] [RecordedDeviceCallID=UInt][GatewayGuid=String][RecordedDeviceDN=String] [RecordingMediaPreference=Enum][CauseValue=UInt][Reason=Enum][AppID=String] [ClusterID=String][NodeID=String]: Recording media resources not available (Phone or Gateway, or Both).

Explanation Phone and/or Gateway resources not available to record call

Recommended Action Determine which recording media resources are eligible to record the call based on the call flow (Phone, Gateway, or Both). Verify configuration of all eligible recording media resources (Phone, Gateway, or Both).

Reason Code - Enum Definitions

Enum Definitions - RecordingMediaPreference

Value	Definition
1	Gateway Preferred
2	Phone Preferred
3	Phone Only

Enum Definitions - Reason

Value	Definition
1	Recording media resources not available (Phone or Gateway)

Error Message

%UC_CALLMANAGER-6-RecordingInvalidCallState: %[RecordedDeviceName=String] [RecordedDeviceCallID=UInt][GatewayGuid=String][RecordedDeviceDN=String] [RecordingMediaPreference=Enum][RecordingMediaSource=Enum][RecordingClusterID=String] [CauseValue=UInt][Reason=Enum][AppID=String][ClusterID=String][NodeID=String]: Invalid Call State; internal error.

Explanation Recording session setup failed

Recommended Action Determine which recording media resources are eligible to record the call based on the call flow (Phone, Gateway, or Both). Verify configuration of all eligible recording media resource (Phone, Gateway, or Both). If Cluster ID is displayed under AlarmValue, check SIP trunk configuration and gateway registration on other cluster.

Reason Code - Enum Definitions

Enum Definitions - RecordingMediaPreference

Value	Definition
1	Gateway Preferred
2	Phone Preferred
3	Phone Only

Enum Definitions - RecordingMediaSource

Value	Definition
1	Phone
2	Gateway

Enum Definitions - Reason

Value	Definition
1	Invalid Call State; internal error

Error Message

%UC_CALLMANAGER-6-RecordingAlreadyInProgress: %[RecordedDeviceName=String] [RecordedDeviceDN=String][RecordedDeviceCallID=UInt][GatewayGuid=String] [RecordingMediaPreference=Enum][RecordingMediaSource=Enum][RecordingClusterID=String] [CauseValue=UInt][Reason=Enum][AppID=String][ClusterID=String][NodeID=String]: Recording session already in progress.

Explanation Recording session setup failed

Recommended Action Determine which recording media resources are eligible to record the call based on the call flow (Phone, Gateway, or Both). Verify configuration of all eligible recording media resource (Phone, Gateway, or Both). If Cluster ID is displayed under AlarmValue, check SIP trunk configuration and gateway registration on other cluster.

Reason Code - Enum Definitions

Enum Definitions - RecordingMediaPreference

Value	Definition
1	Gateway Preferred
2	Phone Preferred
3	Phone Only

Enum Definitions - RecordingMediaSource

Value	Definition
1	Phone
2	Gateway

Enum Definitions - Reason

Value	Definition

1	Recording session already in progress

Error Message

%UC_CALLMANAGER-3-RecordingSessionTerminatedUnexpectedly: %[RecordedDeviceName=String][RecordedDeviceDN=String][RecordingMediaPreference=Enum][RecordingMediaSource=Enum][RecordingDestinationAddress=String][RecordingClusterID=String][RecordedDeviceCallID=UInt][GatewayGuid=String][CauseValue=UInt][Reason=Enum][AppID=String][ClusterID=String][NodeID=String]: Recording session is terminated unexpectedly..

Explanation Recording session setup failed

Recommended Action Check SIP Trunk connected to recording server. Check recording server status. Verify call flow is supported.

Reason Code - Enum Definitions

Enum Definitions - RecordingMediaPreference

Value	Definition
1	Gateway Preferred
2	Phone Preferred
3	Phone Only

Enum Definitions - RecordingMediaSource

Value	Definition
1	Phone
2	Gateway

Enum Definitions - Reason

Value	Definition
1	SIP Trunk to the recording server is out-of-service. Recording server ends session unexpectedly. Call flow not supported

Explanation Recording session setup failed

Recommended Action Check SIP Trunk connected to recording server. Check recording server status. Verify call flow is supported.

Error Message

%UC_CALLMANAGER-4-ILSDuplicateURI: %[URI=String][RouteStrings=String][AppID=String][ClusterID=String][NodeID=String]: Duplicate URI Found in ILS network

Explanation A duplicate URI has been found in this ILS Network.

Recommended Action Check if there are duplicate URI entries learned from remote ILS clusters. Determine which Cisco Unified Communications Manager cluster needs to be changed so that there is no duplicate URI. Reconfigure the remote serves to ensure the URIs configured are unique within a ILS network.

Error Message

%UC_CALLMANAGER-4-CallingNumberNotConfiguredOnCallingDevice: %[CallingNumberNotConfigured=String][DeviceName=String][SourceIPAddress=String][AppID=String][ClusterID=String][NodeID=String]: A call was attempted from a number not configured on this SIP phone

Explanation A call was attempted from a calling number that is not configured on the SIP device. The incoming Calling number did not match any of the configured lines on the device. For security reasons Communications Manager refused the call.

Recommended Action Validate that the IP address from which the call was made matches the current IP address of the device. Reset the device and verify it is able to obtain the correct configuration file from TFTP. Check for a mismatched CTL or ITL file which can prevent the device from accepting the configuration file provided by the TFTP server. This may also be indicative of a security issue in progress; proper investigation is highly recommended

Error Message

%UC_CALLMANAGER-6-CallingLineNumberInconsistenciesCorrected: %[InvalidCallingNumberSentByDevice=String][CallingNumberAfterCorrection=String][DeviceName=String][SourceIPAddress=String][AppID=String][ClusterID=String][NodeID=String]: Inconsistent line numbers found in received SIP headers were corrected.

Explanation The system received SIP headers containing one or more line numbers not configured on this device. The received SIP headers also contain at least one valid line number configured on this device. All calling number information was corrected to be a valid line number before proceeding with call processing.

Recommended Action Validate that the IP address from which the call was made matches the current IP address of the device. Please investigate that the endpoint is behaving as expected. For Cisco devices, reset the device and verify it is able to obtain the correct configuration file from TFTP; if the behavior persists, engage Cisco TAC as necessary.3rd party devices may trigger this Informational alarm if they do not send calling party information in the format expected by Communications Manager. This may also be indicative of a security issue in progress; proper investigation is highly recommended.

Error Message

%UC_CALLMANAGER-6-ExternalQoSTokenAvailable: %[APIC-EM IP=String][AppID=String] [ClusterID=String][NodeID=String]: Access Token from APIC-EM is available

Explanation CUCM was able to get the access token from APIC-EM successfully.

Recommended Action This alarm is for informational purposes only; no action is required.

Error Message

%UC_CALLMANAGER-3-ExternalQoSTokenUnavailable: %[APIC-EM IP=String][AppID=String] [ClusterID=String][NodeID=String]: Unable to get Access Token from APIC-EM

Explanation CUCM requires valid Access Token to exchange REST API's with APIC-EM for policy update. This Access Token is not available from APIC-EM due to authentication or network error

Recommended Action Check the network connectivity between CUCM and APIC-EM. Confirm if the User name and password configured in HTTP Profile page matches with the policy admin credentials in APIC-EM. Once corrected, toggle the "External QoS enabled" parameter in Service parameter to false and then to true.

Error Message

%UC_CALLMANAGER-6-ParkingLotCdpcLeak: %[ProcessName=String][NodeId=UInt][AppId=UInt] [ProcessNumber=UInt][ProcessInstance=UInt][AppID=String][ClusterID=String] [NodeID=String]: Possible leak of ParkinglotCdpc found

Explanation Possible old stuck calls with ParkingLotCdpc. This may happen if CUCM wraps up the CI, after CI gets exhausted.

Recommended Action Informational purposes only; no action is required. Problem was caught and resolved .

Error Message

%UC_CALLMANAGER-1-PushNotificationServiceUnavailable: %[Type=String] [CPNSPortNumber=String][AppID=String][ClusterID=String][NodeID=String]: Unable to connect with local Cisco Push Notification Service (CPNS)

Explanation The Cisco CallManager service requires a connection with CPNS to send Push Notifications to the Cisco Collaboration Cloud. The connection with CPNS is not established or has been lost due to a service error.

Recommended Action Check if the Cisco Push Notification Service is running. If the CPNS is not running, start it. If it is already running, try re-starting the service.

Error Message

%UC_CALLMANAGER-3-PushNotificationInvalidDeviceTokenResponse: %[Type=String] [DevicePkid=String][DeviceName=String][TrackingId=String][PushNotificationResponseText=String]

[AppID=String][ClusterID=String][NodeID=String]: The Cisco Collaboration Cloud returned error code 410 in response to a Push Notification sent from the Cisco CallManager service.

Explanation The push notification sent from the Cisco CallManager Service to the Cisco Collaboration Cloud returned an error due to an invalid device token. Until a valid device token is sent by this iOS Jabber device it will no longer receive push notifications.

Recommended Action The user must log out and log back in to the Jabber client on the iOS device.

Error Message

%UC_CALLMANAGER-1-PushNotificationServiceAccessTokenUnavailable: %[Type=String] [Reason=Enum][ErrorText=String][TrackingId=String][AppID=String][ClusterID=String] [NodeID=String]: Cisco Push Notification Service (CPNS) does not have a valid Access Token

Enum Definitions - Reason code

Value	Definition
0	Access token is not available due to unknown reason
400	invalid_request, unsupported_grant_type, invalid_client, invalid_refresh_token, tokenlimit_reached
401	invalid refresh_guid
405	Method Not Allowed
413	Payload too large
500	Internal Server Error
503	Service unavailable

Explanation Cisco Unified Communications Manager requires a valid access token to send push notifications to the Cisco Collaboration Cloud. This access token is currently not available due to an authentication or network error.

Recommended Action Check on the Cloud Onboarding page to confirm that the Onboarding process has completed successfully. If the issue persists contact Cisco TAC for further assistance.

Error Message

%UC_CALLMANAGER-3-SecureSIPTrunkExportControlNotAllowed: %[SIPTrunk=String][AppID=String] [ClusterID=String][NodeID=String]: A Secure SIP trunk is provisioned while CUCM Cluster is not entitled for Export Control Compliance

Explanation A SIP trunk is provisioned with an Encrypted SIP Trunk Security Profile or has "SRTP Enabled" but this Unified Communications Manager cluster is not licensed for Export Control functionality.

Recommended Action Remove encryption settings from this SIP Trunk or ensure Smart License registration is completed using the Registration Token received from the Smart/Virtual Account that has "Allow export-controlled functionality" checked.

Error Message

%UC_CALLMANAGER-2-LocalPushNotificationServiceUnavailable: %[Reason=String][Type=String][AppID=String][ClusterID=String][NodeID=String]: Unable to connect with Cisco Local Push Notification service.

Explanation The CallManager service requires a connection in order to send Local Push Notifications to the Webex App on Mobile.

Recommended Action Try restarting Cisco Push Notification service and Cisco Local Push Notification service. If the issue persists check the application logs for the Cisco Local Push Notification service and contact Cisco TAC for further assistance.

Error Message

%UC_CALLMANAGER-6-SSLorTCPConnectionFailure: %[PeerAddr=String][PeerPortNo=Int][ReasonCode=Int][Reason=String][AppID=String][ClusterID=String][NodeID=String]: Unified CM failed to open a TCP/TLS connection for the indicated device

Explanation Unified CM failed to open a TCP/TLS connection for the indicated device due to network issue or certificate not valid

Recommended Action If this is a TLS connection, then please check the necessary certificates have been uploaded on the servers properly,or check the Validity and X.509 name of the certificates are properly configured. If this is a TCP connection, then please check the IP address is reachable or if it is configured.

Error Message

%UC_SERVICEMANAGER-5-ServiceActivated: %[ServiceName=String][AppID=String][ClusterID=String][NodeID=String]: Service Activated..

Explanation This service is now activated.

Recommended Action No action is required.

Error Message

%UC_SERVICEMANAGER-5-ServiceDeactivated: %[ServiceName=String][AppID=String][ClusterID=String][NodeID=String]: Service Deactivated..

Explanation This service is now deactivated.

Recommended Action No action is required.

Error Message

%UC_SERVICEMANAGER-1-ServiceActivationFailed: %[ServiceName=String][Reason=String][ErrorString=String][AppID=String][ClusterID=String][NodeID=String]: Failed to activate a service..

Explanation Failed to activate this service.

Recommended Action Activate the service again

Error Message

%UC_SERVICEMANAGER-1-ServiceDeactivationFailed: %[ServiceName=String][Reason=String][ErrorString=String][AppID=String][ClusterID=String][NodeID=String]: Failed to deactivate a service..

Explanation Failed to deactivate this service.

Recommended Action Deactivate the service again

Error Message

%UC_SERVICEMANAGER-2-ServiceFailed: %[ServiceName=String][ProcessID=Int][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: Service terminated..

Explanation The Service has terminated abruptly. Service Manager will try to restart it.

Recommended Action Monitor the state of the service.

Error Message

%UC_SERVICEMANAGER-2-ServiceStartFailed: %[ServiceName=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: Failed to start service..

Explanation Failed to start this service. Service Manager will attempt to start the service again.

Recommended Action Monitor the state of the service.

Error Message

%UC_SERVICEMANAGER-2-ServiceStopFailed: %[ServiceName=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: Failed to stop service..

Explanation Unable to stop the specified service after serveral retries. The service will be marked stopped.

Recommended Action Check the syslog for system error code.

Error Message

%UC_SERVICEMANAGER-2-ServiceRestartFailed: %[ServiceName=String][Reason=String] [AppID=String][ClusterID=String][NodeID=String]: Failed to Restart service..

Explanation Unable to restart the specified service.

Recommended Action No action is required.

Error Message

%UC_SERVICEMANAGER-1-ServiceExceededMaxRestarts: %[ServiceName=String][RestartCount=Int] [AppID=String][ClusterID=String][NodeID=String]: Service failed to start and exceeded maximum allowed restarts..

Explanation Service failed to start, even after the max restarts attempts.

Recommended Action Start the service manually.

Error Message

%UC_SERVICEMANAGER-0-FailedToReadConfig: %[Filename=String][Reason=String][AppID=String] [ClusterID=String][NodeID=String]: Service Manager failed to read configuration file..

Explanation Failed to read configuration file. Configuration file might be corrupted.

Recommended Action Re-install CUCM

Error Message

%UC_SERVICEMANAGER-1-MemAllocFailed: %[MemAllocFailure=String][AppID=String] [ClusterID=String][NodeID=String]: Memory allocation failed..

Explanation Failure to allocate memory.

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 CUCM node.

Error Message

%UC_SERVICEMANAGER-1-SystemResourceError: %[SystemCall=String][Service=String][Reason=String][AppID=String][ClusterID=String][NodeID=String]: A System call failed..

Explanation System call failed.

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 node.

Error Message

%UC_SERVICEMANAGER-3-ServiceManagerUnexpectedShutdown: %[ProcessID=ULong][ServiceName=String][AppID=String][ClusterID=String][NodeID=String]: Service Manager restarted successfully after an unexpected termination..

Explanation Service Manager unexpectedly terminated. Service Manager has recovered but other components may be adversely affected. The only known causes of unexpected termination are adverse conditions such as hard power down, kernel panic, and readonly filesystem caused due to hardware or software. These conditions can corrupt the filesystem and database in ways that are unrecoverable. Repeat occurrences inevitably lead to corruption. It is critical to identify and remedy the cause of this unexpected termination.

Recommended Action Always shutdown via CLI or platform UI. Do not yank the power-cord or press and hold the power button. Use the recovery disk to perform a filesystem check to identify and attempt to correct any errors that occurred. If errors are detected a rebuild and restore from backup is recommended. Use a redundant reliable power source such as UPS and leverage Uninterruptible Power Supply (UPS) Integration for Unified CM. Run hardware diagnostics to check for hardware failures. If unexpected terminations persist contact Cisco Technical Support for assistance.

Error Message

%UC_CWLCSS-5-SwitchesAndAccessPointReached75PercentCapacity: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: The current record count for switches and access points has reached 75%. The maximum capacity is 50000.

Explanation The current record count for switches and access points has reached 75%. The maximum capacity is 50000.

Recommended Action Please review number of switches and access points and their activation status. Ensure the count is kept below this threshold to avoid service shutdown.

Error Message

%UC_CWLCSS-4-SwitchesAndAccessPointReached90PercentCapacity: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: The current record count for switches and access points has reached 90%. The maximum capacity is 50000.

Explanation The current record count for switches and access points has reached 90%. The maximum capacity is 50000.

Recommended Action Please review number of switches and access points and their activation status. Ensure the count is kept below this threshold to avoid service shutdown.

Error Message

%UC_CWLCSS-4-SwitchesAndAccessPointReached95PercentCapacity: %[Reason=String] [AppID=String][ClusterID=String][NodeID=String]: The current record count for switches and access points has reached 95%. The maximum capacity is 50000.

Explanation The current record count for switches and access points has reached 95%. The maximum capacity is 50000.

Recommended Action Please review number of switches and access points and their activation status. Ensure the count is kept below this threshold to avoid service shutdown.

Error Message

%UC_CWLCSS-1-CiscoWLCSyncServiceDown: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: Reached maximum record count for Switches and Access Points. The maximum capacity is 50000.

Explanation Exceeded maximum number of devices in the Switches and Access points. The maximum capacity is 50000.

Recommended Action You need to review current set of switches and access points for their activation status. Delete unused devices to ensure sufficient capacity and restart service.

Error Message

%UC_CWLCSS-6-CiscoWLCSyncStarted: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: Cisco WLC Synchronization service successfully started.

Explanation Application successfully started.

Recommended Action No action required.

Error Message

%UC_CWLCSS-6-CiscoWLCSyncStartFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: Cisco WLC Synchronization service failed to start.

Explanation Error occurred while starting application.

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

Error Message

%UC_CWLCSS-3-CiscoWLCSyncDBAccessFailure: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: CiscoWLCSync process failed to access local database.

Explanation CiscoWLCSync failed to access local database.

Recommended Action Please make sure the local CallManager database is working properly. The failed sync process will restart at the next scheduled time.

Error Message

%UC_CWLCSS-3-CiscoWLCSyncDBInsertFailure: %[Reason=String][AppID=String][ClusterID=String] [NodeID=String]: CiscoWLCSync process cannot insert a new record.

Explanation Exceeded maximum number of devices in the Switches and Access points.

Recommended Action You need to review current set of switches and access points for their activation status. Delete unused devices to ensure sufficient capacity.

Error Message

%UC_CWLCSS-6-CiscoWLCSyncProcessStarted: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: Cisco WLC synchronization process started on particular WLC.

Explanation Cisco WLC synchronization process started to sync Access Point(AP) data for the configured WLC.

Recommended Action No action required.

Error Message

%UC_CWLCSS-3-CiscoWLCSyncProcessFailToStart: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: CiscoWLCSync process failed to start on particular WLC.

Explanation CiscoWLCSync process failed to start on the configured WLC.

Recommended Action See application logs for error.

Error Message

%UC_CWLCSS-6-CiscoWLCSyncProcessCompleted: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: CiscoWLCSync process completed on particular WLC.

Explanation CiscoWLCSync process completed Access Point(AP) data sync for the configured WLC.

Recommended Action No action required.

Error Message

%UC_CWLCSS-6-CiscoWLCSyncProcessStoppedManually: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: CiscoWLCSync process stopped manually on particular WLC.

Explanation CiscoWLCSync process stopped manually on the configured WLC.

Recommended Action SNo action required.

Error Message

%UC_CWLCSS-6-CiscoWLCSyncNoSchedulesFound: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: No schedules found in DB for WLC synchronization.

Explanation No automatic WLC synchronization possible.

Recommended Action Check the WLC configuration.

Error Message

%UC_CWLCSS-6-CiscoWLCSyncInvalidScheduleFound: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: Invalid schedule read by CiscoWLCSync scheduler from database.

Explanation Invalid schedule read by CiscoWLCSync scheduler from database.

Recommended Action Check the WLC configuration and logs.

Error Message

%UC_CWLCSS-3-CiscoWLCSyncSNMPResponseTimeout: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: CiscoWLCSync process SNMP request timed out.

Explanation CiscoWLCSync process SNMP request timed out.

Recommended Action Please make sure the WLC server is available and configured to allow SNMP query from the UCM server.

Error Message

%UC_CWLCSS-3-CiscoWLCSyncSNMPv2CommunityStringError: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: SNMP Community string is incorrect for WLC.

Explanation Community string specified for the WLC is incorrect.

Recommended Action Please verify the community string for the WLC.

Error Message

%UC_CWLCSS-3-CiscoWLCSyncSNMPv3AuthenticationError: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: SNMPv3 Authentication is incorrect for WLC.

Explanation The SNMPv3 Authentication failed.

Recommended Action Please ensure SNMP User Id, SNMP authentication protocol and password, SNMP privacy protocol and password are specified correctly.

Error Message

%UC_CLUSTERMANAGER-6-CLM_IPSecCertUpdated: %[NodeName=String][AppID=String] [ClusterID=String][NodeID=String]: IPSec self-signed cert updated. .

Explanation The IPSec self-signed cert from a peer node in the cluster has been imported due to a change.

Recommended Action No action is required.

Error Message

%UC_CLUSTERMANAGER-6-CLM_IPAddressChange: %[NodeName=String][NodeOldIP=String] [NodeNewIP=String][AppID=String][ClusterID=String][NodeID=String]: IP address change in cluster. .

Explanation The IP address of a peer node in the cluster has changed.

Recommended Action No action is required.

Error Message

%UC_CLUSTERMANAGER-1-CLM_PeerState: %[NodeName=String][NodeState=String] [AppID=String][ClusterID=String][NodeID=String]: Current ClusterMgr session state..

Explanation The ClusterMgr session state with another node in the cluster has changed to the current state.

Recommended Action No action is required.

Error Message

%UC_CLUSTERMANAGER-1-CLM_MsgIntChkError: %[NodeIP=String][AppID=String] [ClusterID=String][NodeID=String]: ClusterMgr message integrity check error. .

Explanation 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.

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

Error Message

%UC_CLUSTERMANAGER-3-CLM_UnrecognizedHost: %[NodeIP=String][AppID=String][ClusterID=String][NodeID=String]: ClusterMgr unrecognized host..

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

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

Error Message

%UC_CLUSTERMANAGER-1-CLM_ConnectivityTest: %[NodeIP=String][ErrorString=String][AppID=String][ClusterID=String][NodeID=String]: CLM Connectivity Test Failed. .

Explanation Cluster Manager detected a network error.

Recommended Action Verify connectivity between cluster nodes and fix any network issues.

Error Message

%UC_AUDITEVENT-4-AuditLogsExceedsConfiguredThreshold: %[AppID=String][ClusterID=String][NodeID=String]: Indicates that the disk space configured for application audit logging exceeds the configured threshold.

Explanation This alarm indicates the percentage of disk space configured for application audit logging exceeds the configured threshold. Audit logs files will be overwritten sooner or later depends on the frequency of audit logging by the CUCM applications.

Recommended Action Login to " Cisco Unified Serviceability - > Tools - > Audit Log Configuration " and check the notification settings for application audit log. If the Warning Threshold for Approaching Log Rotation Overwrite is set to a lower value than the default(80%) threshold unintentionally, set it to default. Please contact Cisco Technical Assistance Centre (TAC) for further support.

Error Message

%UC_AUDITEVENT-4-AuditLogOverFlowDueToLogRotation: %[AppID=String][ClusterID=String][NodeID=String]: AuditLogOverFlowDueToLogRotation

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

Recommended Action Login to " Cisco Unified Serviceability - > Tools - > Audit Log Configuration " and check if the Audit Log Rotation is enabled. Administrator can choose not to overwrite the audit log files by disabling the " Enable Log Rotation " option.Please contact Cisco Technical Assistance Centre (TAC) for further support.

Error Message

%UC_PHONE-6-DeviceImageDownloadStart: %[DeviceName=String][IPAddress=String] [Active=String][RequestedLoadId=String][AppID=String][ClusterID=String][NodeID=String]: Device has begun downloading the firmware load

Explanation Cisco IP Phone has started downloading its firware load (image)

Recommended Action Informational purposes only; no action is required

Error Message

%UC_PHONE-6-DeviceImageDownloadSuccess: %[DeviceName=String][IPAddress=String] [Method=Enum][Active=String][InActive=String][Server=String][AppID=String][ClusterID=String] [NodeID=String]: Device has successfully downloaded the firmware load

Explanation Cisco IP Phone has successfully downloaded its image.

Recommended Action No action is required.

Method - Method used for downloading the device firmware

Enum Definitions - Method

Value	Definition
0	
1	TFTP
2	HTTP
3	PPID

Error Message

%UC_PHONE-4-DeviceImageDownloadFailure: %[DeviceName=String][IPAddress=String] [Active=String][InActive=String][FailedLoadId=String][Method=Enum][FailureReason=Enum] [Server=String][AppID=String][ClusterID=String][NodeID=String]: Device firmware download has failed

Explanation Cisco IP phone failed to download its firmware load (image) for the reason defined in this alarm

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.

Method - Method used for downloading the device firmware

Enum Definitions - Method

Value	Definition
0	
1	TFTP
2	HTTP

3	PPID

FailureReason - Reason that the firmware load has failed to download

Enum Definitions - FailureReason

Value	Definition
0	
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's 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
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's 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.
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 superceded by a new download request. The original download was cancelled so that the new download could continue. No action is required.

Error Message

%UC_PHONE-6-DeviceApplyConfigResult: %[DeviceName=String][IPAddress=String] [CUCM_Result=Enum][Phone_Result=Enum][Reason=Enum][AppID=String][ClusterID=String] [NodeID=String]: Indicates the result of an Apply Config action in Unified CM Administration

Explanation Cisco IP Phone has applied its config

Recommended Action No action is required.

CUCM_Result - UnifiedCM_Result

Enum Definitions - CUCM_Result

Value	Definition
0	
1	no change - the new phone configuration changes do not impact Unified CM.
2	Configuration changes applied - The Unified CM Administration applied the configuration changes dynamically without requiring phone to re-register.
3	Re-registration - The Unified CM Administration applied the configuration changes and required the phone to re-register to make them effective.

Phone_Result - Phone_Result

Enum Definitions - Phone_Result

Value	Definition
0	
1	Configuration changes applied - The phone applied the configuration changes dynamically without a reset or restart.
2	Reset delayed - Phone will set the inactive partition as active partition, then reset, and come

	up from the new active partition.
3	Restart now - The phone will restart immediately.
4	Restart delayed - The phone will restart, but restart is delayed for reason as specified in reason parameter.
5	Config pending- The phone will delay applying the configuration changes because phone is downloading a firmware image.
6	TFTP Error- While downloading the configuration file, phone encountered tftp error for reason as specified in reason parameter .

Reason - Reason

Enum Definitions - Reason

Value	Definition
0	
1	Configuration file changed- Config file has changed since last download of configuration file.
2	Download in progress- Download of firmware image is going on.
3	Call is active- A call is active on the phone.
4	Re-registration delayed - Because call is active, re-registration of the phone is delayed. Registration will resume when phone is idle.
5	Reset delayed - Because call is active, reset of phone is

	delayed. Reset will continue when phone is idle.
6	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 configuration file and correct any TFTP errors that may have occurred. Also, investigate the configuration file on the TFTP server to ensure that configuration file requests are being processed; check network connectivity to the TFTP server.
7	Specified configuration file is not found on the TFTP server. Check that file name is correct and file exist on TFTP server.
8	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
9	An internal phone error occurred during the download attempt of configuration file; reset the phone to correct the issue
10	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 configuration file, 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 configuration file, 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.
11	Specified CTL file is not found on the TFTP server. Check that file name is correct and file exist on TFTP server.
12	Authentication for CTL file failed; reset the phone to correct the issue
13	The Load server or TFTP server could not process the phone's configuration file download request. It's 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 configuration file again. If resetting the phone does not solve the issue, restart the Load server or TFTP server (whichever server provides configuration file).

14	An encryption error occurred on the phone while trying to load the new configuration file; reset the phone to correct the issue
15	The downloaded configuration file is not encrypted. Verify that security or authentication mode of phone is same as what is configured in Unified CM for that phone and that the server that provides configuration file has that encrypted file
16	The downloaded configuration file cannot be decrypted using the decryption key on the phone (resulting in an encryption key mismatch). If you have provided the configuration file encryption key, try re-encrypting the configuration file 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).
17	There is a problem with the encryption of the downloaded configuration file. Collect pertinent details such as the device's MAC address, device type, the configuration file, 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).
18	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 configuration file. 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).
19	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.
20	An internal phone error occurred in processing the configuration file; restart the phone to correct the issue
21	Configuration file Re-TFTP - Phone need to download the configuration file again.

22	Certification mismatch for configuration file - Phone detected certification mismatch for downloaded configuration file.
23	Firmware load update required - Phone need to download new firmware image.

Error Message

%UC_PHONE-4-DeviceConfigFailure: %[DeviceName=String][IPAddress=String] [CurrentConfigVersionStamp=String][NewConfigVersionStamp=String][FailureReason=Enum] [AppID=String][ClusterID=String][NodeID=String]: Device was unable to install the new configuration file

Explanation Cisco IP Phone is unable to install the latest configuration file. After a configuration change has occurred in Cisco Unified CM Administration, the phone successfully downloads its new configuration file but due to some error, it cannot install it.

Recommended Action Refer to the reason code descriptions for recommended actions

FailureReason - Failure reason

Enum Definitions - FailureReason

Value	Definition
0	
1	Version mismatch - The version of the configuration file that was downloaded does not match the version stamp of the file that was requested by Unified CM. The phone failed to load the file due to the version stamp mismatch. This sometimes occurs due to a misstep during a phone or Unified CM upgrade. Verify that database replication is functioning by going to the Cisco Unified Reporting web page, generating a Unified CM Database Status report, and verifying that "all servers have a good replication status". 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. If replication is not working, restart the TFTP and Cisco CallManager services.
2	TFTP server unavailable – Either the IP address of the TFTP server configured in the Administrator Settings is incorrect or the TFTP server is not running. Verify that phone settings have the correct TFTP IP address and that the TFTP server is running.
3	File not found – The phone configuration file requested by the phone does not exist in the TFTP server. Verify that IP address provided in the Administration Setting for TFTP server is correct. Verify that the phone is configured in Unified CM Administration and the MAC address shown in Unified CM Administration matches the actual MAC address of the phone. If the phone is not configured in Unified CM Administration, configure the phone in Unified CM Administration and manually restart the phone from the administrator settings on the device itself.
4	Read error – The phone is unable to read the configuration file successfully. 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).

Error Message

%UC_PHONE-4-PowerSavePlusFailure: %[DeviceName=String][DeviceIPv4Address=String][Reason=Enum][AppID=String][ClusterID=String][NodeID=String]: The device could not enter Power Save Plus

Explanation The device indicated in this alarm could not enter Power Save Plus mode, even though the feature is enabled for this device. This can occur because of configuration errors such as a missing or incorrect EneergyWise domain or secret, a power supply to the device that is incompatible with the Power Save Plus feature, or because the switch is not EnergyWise enabled or has refused to allow the device to enter Power Save Plus mode

Recommended Action Actions to correct this condition vary according to the reason code specified in this alarm. Refer to the reason code definitions in this alarm for recommended actions

Reason - Reason

Enum Definitions - Reason

Value	Definition
0	
1	NoEnergyWiseDomain - The EnergyWise domain has not been configured on this device. An EnergyWise domain is always required for the Power Save Plus feature even when the Allow EnergyWise Overrides check box is not checked. Specify an EnergyWise domain on the Device Configuration window in Unified CM Administration, in the EnergyWise Domain field
2	>NoEnergyWiseSecret - The EnergyWise secret (password) has not been configured on this device. An EnergyWise secret is always required for the Power Save Plus feature even when the Allow EnergyWise Overrides check box is not checked. Specify an EnergyWise secret on the

	Device Configuration window in Unified CM Administration, in the EnergyWise Secret field
3	NoEnergyWiseSecret - The EnergyWise secret (password) has not been configured on this device. An EnergyWise secret is always required for the Power Save Plus feature even when the Allow EnergyWise Overrides check box is not checked. Specify an EnergyWise secret on the Device Configuration window in Unified CM Administration, in the EnergyWise Secret field
4	NoEnergyWiseSwitch - The device is not attached to a switch that has EnergyWise enabled. This can occur if the device is attached to a Cisco switch but EnergyWise has not been enabled or if the EnergyWise-enabled switch is running a Cisco IOS version that is incompatible with the Power Save Plus feature. Verify that the device is attached to a Cisco switch that has EnergyWise enabled and that the version of the IOS software that the switch is running includes support for the EnergyWise/Power Save Plus feature
5	PSPRejected - The EnergyWise-enabled switch refused to allow the device to enter Power Save Plus. Verify that the version of the IOS software that the switch is running includes support for the EnergyWise/Power Save

	Plus feature. Examine the switch and the reject message (negative acknowledgement) for any information relating to the reason for the refusal

Error Message

%UC_PHONE-6-LastOutOfServiceInformation: %[DeviceName=String][DeviceIPv4Address=String] [IPv4DefaultGateway=String][DeviceIPv6Address=String][IPv6DefaultGateway=String] [ModelNumber=String][NeighborIPv4Address=String][NeighborIPv6Address=String] [NeighborDeviceID=String][NeighborPortID=String][VoiceVLAN=String][UnifiedCMIPAddress=String] [LocalPort=String][TimeStamp=String][LastProtocolEventSent=String] [LastProtocolEventReceived=String][DHCPv4Status=Enum][DHCPv6Status=Enum] [TFTPCfgStatus=Enum][DNSStatusUnifiedCM1=Enum][DNSStatusUnifiedCM2=Enum] [DNSStatusUnifiedCM3=Enum][DNSv6StatusUnifiedCM1=Enum][DNSv6StatusUnifiedCM2=Enum] [DNSv6StatusUnifiedCM3=Enum][ReasonForOutOfService=Enum][AppID=String][ClusterID=String] [NodeID=String]: Information related to the last out-of-service event

Explanation The device has lost communication with Unified CM, due to a reason such as a network connectivity issue, Unified CM outage, configuration error, and in some cases, a normal unregistration event. A device can go out-of-service for many reasons, both intentional such as manually resetting the device after a configuration change, and unintentional such as loss of network connectivity. Other causes for this alarm could include a device being registered to a secondary node and then the primary node coming online, which causes the device to re-home to the primary Unified CM node. Other error conditions include lack of a KeepAlive being returned from the Unified CM node to which this device was registered, and so on.

Recommended Action A Actions to take vary depending on the reason specified in this alarm for why the device went out of service. If the device being out of service is expected (normal occurrence), such as during a manual devie reset, no action is required. Reason codes 18-23 are all normal reason codes. Other reason codes should be investigated to determine why Unified CM is not running or whether a network problem or configuration error exists. In the case of a network connectivity problem or loss of KeepAlives, use network diagnostic tools, the Real-Time Monitoring Tool, and the Cisco Unified CM Reporting tool to evaluate and correct any reported network or Unified CM system errors. In the case of a device re-homing to the primary Unified CM node, watch for a successful registration of the device on the primary node. Also, refer to the reason code descriptions for recommended actions

DHCPv4Status - DHCPv4Status

Enum Definitions - DHCPv4Status

Value	Definition
0	
1	Successful - DHCPv4 configuration completed without error
2	Successful - DHCPv4 configuration completed without error

3	Successful - DHCPv4 configuration completed without error

DHCPv6Status - DHCPv6Status

Enum Definitions - DHCPv6Status

Value	Definition
0	
1	Successful - DHCPv6 configuration completed without error
2	RequestTimedOut - The DHCPv6 request timed out. Check for and correct errors on the DHCP server
3	DHCPdisabled - DHCPv6 was disabled at the time the device went out-of-service

TFTPCfgStatus - TFTP Configuration Status

Enum Definitions - TFTPCfgStatus

Value	Definition
0	
1	TFTPDownloadSuccess - TFTP download of the configuration file completed without error
2	TFTPtimedOut - Connection to the TFTP server has timed out - The device attempted to connect to the TFTP server but could not connect successfully. Check the TFTP server IP address as configured in the settings on the device; make sure the IP address is accurate. If it is not, correct the IP address and press Apply; the device should

	restart automatically. Also, verify that network connectivity exists between the device and the TFTP server. Restart the device to attempt connection again unless the restart occurs automatically
3	NoServerInfo – The device did not receive a TFTP IP address or the DNS name was not resolved and as a result, does not have the server information needed to download a configuration file. Check that DHCP option 150 has been configured properly. If the information is inaccurate or not present, supply the correct information and restart the device. If the information is accurate, restart the device. If this alarm recurs, contact the Cisco Technical Assistance Center (TAC)

DNSStatusUnifiedCM1 – DNSv4 Status on Unified CM 1

Enum Definitions – DNSStatusUnifiedCM1

Value	Definition
0	
1	DNSsuccessful – DNS resolution completed without error
2	DNSrequestTimedOut – The DNS request timed out. Check the DNS server and make sure that it is functioning properly
3	DNShostNameNotFound – The DNS server was unable to resolve the host name specified for the primary Cisco Unified CM

4	DNSresolutionNotNeeded – The primary Cisco Unified CM was specified by an IPv4 address so no DNS resolution was needed

DNSStatusUnifiedCM2 – DNSv4 Status on Unified CM 2

Enum Definitions – DNSStatusUnifiedCM2

Value	Definition
0	
1	DNSsuccessful – DNS resolution completed without error
2	DNSrequestTimedOut – The DNS request timed out. Check the DNS server and make sure that it is functioning properly
3	DNShostNameNotFound – The DNS server was unable to resolve the host name specified for the secondary Cisco Unified CM
4	DNSresolutionNotNeeded – The secondary Cisco Unified CM was specified by an IPv4 address so no DNS resolution was needed

DNSStatusUnifiedCM3 – DNSv4 Status on Unified CM 3

Enum Definitions – DNSStatusUnifiedCM3

Value	Definition
0	
1	DNSsuccessful – DNS resolution completed without error

2	DNSrequestTimedOut – The DNS request timed out. Check the DNS server and make sure that it is functioning properly
3	DNShostNameNotFound – The DNS server was unable to resolve the host name specified for the tertiary Cisco Unified CM
4	DNSresolutionNotNeeded – The tertiary Cisco Unified CM was specified by an IPv4 address so no DNS resolution was needed

DNSv6StatusUnifiedCM1 – DNSv6 Status on Unified CM 1

Enum Definitions – DNSv6StatusUnifiedCM1

Value	Definition
0	
1	DNSsuccessful – DNS resolution completed without error
2	DNSrequestTimedOut – The DNS request timed out. Check the DNS server and make sure that it is functioning properly
3	DNShostNameNotFound – The DNS server was unable to resolve the host name specified for the primary Cisco Unified CM
4	DNSresolutionNotNeeded – The primary Cisco Unified CM was specified by an IPv6 address so no DNS resolution was needed

DNSv6StatusUnifiedCM2 – DNSv6 Status on Unified CM 2

Enum Definitions – DNSv6StatusUnifiedCM2

Value	Definition
0	
1	DNSsuccessful – DNS resolution completed without error
2	DNSrequestTimedOut – The DNS request timed out. Check the DNS server and make sure that it is functioning properly
3	DNShostNameNotFound – The DNS server was unable to resolve the host name specified for the secondary Cisco Unified CM
4	DNSresolutionNotNeeded – The secondary Cisco Unified CM was specified by an IPv6 address so no DNS resolution was needed

DNSv6StatusUnifiedCM3 – DNSv6 Status on Unified CM 3

Enum Definitions – DNSv6StatusUnifiedCM3

Value	Definition
0	
1	DNSsuccessful – DNS resolution completed without error
2	DNSrequestTimedOut – The DNS request timed out. Check the DNS server and make sure that it is functioning properly
3	DNShostNameNotFound – The DNS server was unable to resolve the host name specified for the tertiary Cisco Unified CM
4	DNSresolutionNotNeeded – The tertiary Cisco Unified CM

	was specified by an IPv6 address so no DNS resolution was needed

ReasonForOutOfService - Reason For Out Of Service

Enum Definitions - ReasonForOutOfService

Value	Definition
0	
10	TCPtimedOut - The TCP connection to the Cisco Unified Communication Manager experienced a timeout error
12	TCPucmResetConnection - The Cisco Unified Communication Manager reset the TCP connection
13	TCPucmAbortedConnection - The Cisco Unified Communication Manager aborted the TCP connection
14	TCPucmClosedConnection - The Cisco Unified Communication Manager closed the TCP connection
15	SCCPKeepAliveFailure - The device closed the connection due to a SCCP KeepAlive failure
16	TCPdeviceLostIPAddress - The connection closed due to the IP address being lost. This may be due to the DHCP Lease expiring or the detection of IP address duplication. Check that the DHCP Server is online and that no duplication has been reported by the DHCP Server
17	TCPDeviceRegsistrationTimedOut - The device closed the TCP connection due to a registration timeout
18	TCPclosedConnectHighPriorityUcm - The device closed the TCP connection in order to reconnect to a higher priority Cisco Unified CM

20	TCPclosedUserInitiatedReset – The device closed the TCP connection due to a user initiated reset
22	TCPclosedUcmInitiatedReset – The device closed the TCP connection due to a reset command from the Cisco Unified CM
23	TCPclosedUcmInitiatedRestart – The device closed the TCP connection due to a restart command from the Cisco Unified CM
24	TCPClosedRegistrationReject – The device closed the TCP connection due to receiving a registration rejection from the Cisco Unified CM
25	RegistrationSuccessful – The device has initialized and is unaware of any previous connection to the Cisco Unified CM
26	TCPclosedVlanChange – The device closed the TCP connection due to reconfiguration of IP on a new Voice VLAN
30	TCPclosedAlarmWipe – The device closed the TCP connection due to alarm got wiped
31	TCPclosedFileAuthFail – The device closed the TCP connection due to device got locked
32	TCPclosedPowerSavePlus – The device closed the TCP connection in order to enter Power Save Plus mode
33	BatteryDrainPowerOff – Battery drain to gracefully power off
41	TCPclosedDHCPTimeout – The device closed the TCP connection due to DHCP timeout
100	ConfigVersionMismatch – The device detected a version stamp mismatch

	during registration Cisco Unified CM
101	ConfigiFileVersionMismatch – The device detected a version stamp mismatch with config file during registration Cisco Unified CM
104	TCPclosedApplyConfig – The device closed the TCP connection to restart triggered internally by the device to apply the configuration changes
105	TCPclosedDeviceRestart – The device closed the TCP connection due to a restart triggered internally by the device because device failed to download the configuration or dial plan file
106	TCPsecureConnectionFailed – The device failed to setup a secure TCP connection with Cisco Unified CM
107	TCPclosedDeviceReset – The device closed the TCP connection to set the inactive partition as active partition, then reset, and come up from the new active partition
108	VpnConnectionLost – The device could not register to Unified CM because VPN connectivity was lost
109	TCPclosedIPAddressChanged – The device closed the TCP connection due to IP address got changed
111	TCPclosedApplicationRequestedDestroy – The device closed the TCP connection due to Application requested for destroying the connection
113	TCPclosedSocketError – The device closed the TCP connection due to Socket Error
200	ClientApplicationClosed – The device was unregistered because the client application was closed

201	OsInStandbyMode - The device was unregistered because the OS was put in standby mode
202	OsInHibernateMode - The device was unregistered because the OS was put in hibernate mode
203	OsInShutdownMode - The device was unregistered because the OS was shut down
204	ClientApplicationAbort - The device was unregistered because the client application crashed
205	DeviceUnregNoCleanupTime - The device was unregistered in the previous session because the system did not allow sufficient time for cleanup
206	DeviceUnregOnSwitchingToDeskphone - The device was unregistered because the client requested to switch from softphone to deskphone control
207	DeviceUnregOnSwitchingToSoftphone - The device is being registered because the client requested to switch from deskphone control to softphone
208	DeviceUnregOnNetworkChanged - The device is being unregistered because the client detected a change of network
209	DeviceUnregExceededRegCount - The device is being unregistered because the device has exceeded the maximum number of concurrent registrations
210	DeviceUnregExceededLoginCount - The device is being unregistered because the client has exceeded the maximum number of concurrent logons

Error Message

%UC_PHONE-6-DeviceTLInfo: %[DeviceName=String][IPv4Address=String][IPv6Address=String] [CTL_Signature=String][CTL_TFTP_Server=String][ITL_Signature=String][ITL_TFTP_Server=String]

[StatusCode=Enum][AppID=String][ClusterID=String][NodeID=String]: Trust List Files are updated or installed

Explanation Trust List Files(CTL/ITL) are updated or installed. If alarm doesn't have Status_Code parameter, it means the update or installation was successfully. If alarm has this parameter, please check the status code for details.

Recommended Action Informational purposes only; no action is required

StatusCode - StatusCode

Enum Definitions - StatusCode

Value	Definition
0	
1	Update to new CTL and/or ITL success.
2	Update to new CTL success, there was NO existing TL installed on the phone before.
3	Update to new ITL success, there was NO existing TL installed on the phone before.
4	Update to new CTL and ITL success, there was NO existing TL installed on the phone before.
5	Update to new CTL failed, ITL update success, but there was existing TL installed on the phone before.
6	Update to new TL failed, but there was NO existing TL installed on the phone before.
7	Generic failure, connection lost, server busy, invalid parameters and others cause the update operation fail.
8	Update to new ITL failed, CTL update success, but there was existing TL installed on the phone before.
9	Update to new TL failed, but there was existing TL installed

	on the phone before.

Error Message

%UC_PHONE-6-NotSupportAlarm: %[DeviceName=String][DeviceIPv4Address=String] [DeviceIPv6Address=String][DeviceIPAddressingMode=String][DeviceIPv4StackState=String] [DeviceIPv6StackState=String][DeviceNotSupport=String][AppID=String][ClusterID=String] [NodeID=String]: The device does not support the feature

Explanation This alarm is reporting which feature is not supported by the device. e.g. The VPN is not supported in IPv6-only mode. The EMCC is not supported in IPv6-only mode. The PFS is not supported in IPv6-only mode.

Recommended Action Informational purposes only; no action is required

Error Message

%UC_PHONE-6-SendLogsResult: %[DeviceName=String][IPv4Address=String][IPv6Address=String] [StopReason=String][AppID=String][ClusterID=String][NodeID=String]: Send logs to remote log server unsuccessfully

Explanation Send logs to remote log server unsuccessfully

Recommended Action Informational purposes only; no action is required

Error Message

%UC_PHONE-1-APNSAlarm: %[Type=String][DeviceName=String][DevicePkid=String] [IssueDescription=String][AppID=String][ClusterID=String][NodeID=String]: Jabber on IOS device encountered an issue processing a Push Notification

Explanation An iOS Jabber client was unable to process an Push Notification.

Recommended Action Contact Cisco TAC for further assistance.

Error Message

%UC_CPNS-2-StartFailed: %[Reason=String][Type=String][AppID=String][ClusterID=String] [NodeID=String]: A failure occured while starting the service.

Explanation An internal failure is preventing the Cisco Push Notification Service from starting.

Recommended Action Try restarting Cisco Push Notification service. If the issue persists check the application logs for the CPNS service and contact Cisco TAC for further assistance.

Error Message

%UC_CPNS-1-AccessTokenInvalid: %[Type=String][TrackingID=String][ReasonCode=String] [Reason=String][AppID=String][ClusterID=String][NodeID=String]: The current access token has expired and a new access token is not available.

Explanation This alarm indicates that current access token is expired or has become invalid and the token refresh process has not been successful.

Recommended Action Verify that the Cloud Onboarding is completed on Cloud Onboarding page. If using an HTTP Proxy verify the configuration on the Cloud Onboarding page.

Error Message

%UC_CPNS-1-HttpClientPoolCreationError: %[Reason=String][Type=String][AppID=String][ClusterID=String][NodeID=String]: Indicates an error in creating the Http Client connection pool.

Explanation This alarm indicates that creation of the Http Client connection pool encountered an error.

Recommended Action On the Cisco Cloud Onboarding Configuration page verify any HTTP proxy settings are correct and that the on-boarding process has completed. Try restarting the Cisco Push Notification Service.

Error Message

%UC_SLMALARMCATALOG-4-SmartLicenseInEval: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: The system is operating in Evaluation Mode that will expire soon.

Explanation The system is not registered with Cisco Smart Software Manager or satellite and is operating in Evaluation Mode.

Recommended Action Register the system with Cisco Smart Software Manager or satellite.

Error Message

%UC_SLMALARMCATALOG-2-SmartLicenseNoProvision_EvalExpired: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: The license evaluation period has expired.

Explanation The license evaluation period has expired.

Recommended Action Register the system with Cisco Smart Software Manager or satellite in order to restore the ability to provision users and devices.

Error Message

%UC_SLMALARMCATALOG-1-SmartLicenseInOverage_AuthorizationExpired: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: The license authorization has expired.

Explanation The system has not communicated with Cisco Smart Software Manager or satellite for 90 days and the overage period is active. Provisioning of users and devices will not be allowed if a successful license authorization renewal is not done within the overage days left.

Recommended Action Please check the network connection and renew the license authorization to avoid losing the ability to provision users and devices.

Error Message

%UC_SLMALARMCATALOG-2-SmartLicenseNoProvision_AuthorizationExpired: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: The license authorization has expired.

Explanation The system has not communicated with Cisco Smart Software Manager or satellite for 90 days and the system has not automatically renewed the entitlement authorizations. Provisioning of users and devices is no longer allowed.

Recommended Action Please check the network connection and renew the license authorization in order to restore the ability to provision users and devices.

Error Message

%UC_SLMALARMCATALOG-3-SmartLicenseRegistrationExpired: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: The license registration has expired and the system is unregistered with Cisco Smart Software Manager or satellite.

Explanation The current time is outside the valid registration period in the ID certificate and the license registration has expired. This could be caused by a change in the system clock or multiple communication failures with Cisco Smart Software Manager or satellite.

Recommended Action Please check the network connectivity to Cisco Smart Software manager or satellite. Also verify your system clock is correct and then register the system with Cisco Smart Software Manager or satellite. If the operation still fails, use RTMT to collect traces for Cisco Smart License Manager. Alternately, use CLI to collect traces by running the command file get activelog /cm/trace/slm/log4j/. If you are unable to resolve the issue contact TAC for assistance.

Error Message

%UC_SLMALARMCATALOG-1-SmartLicenseInOverage_OutOfCompliance: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: The system is operating with an insufficient number of licenses.

Explanation The system is operating with an insufficient number of licenses and the overage period is active.

Recommended Action Configure additional licenses in Cisco Smart Software Manager to avoid losing the ability to provision users and devices.

Error Message

%UC_SLMALARMCATALOG-2-SmartLicenseNoProvision_OutOfCompliance: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: The system is operating with an insufficient number of licenses.

Explanation The system is operating with an insufficient number of licenses. Configure additional licenses in Cisco Smart Software Manager in order to restore the ability to provision users and devices.

Recommended Action Configure additional licenses in Cisco Smart Software Manager in order to restore the ability to provision users and devices.

Error Message

%UC_SLMALARMCATALOG-3-SmartLicenseCommunicationError: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: The system failed to communicate with Cisco Smart Software Manager or satellite.

Explanation The system is unable to communicate successfully with Cisco Smart Software Manager or satellite.

Recommended Action Please verify that the system has network connectivity to Cisco Smart Software Manager or satellite. If you are unable to resolve the issue contact TAC for assistance.

Error Message

%UC_SLMALARMCATALOG-4-SmartLicenseRegistrationExpiringSoon: %[Reason=String] [AppID=String][ClusterID=String][NodeID=String]: The registration with Cisco Smart Software Manager or satellite will expire soon.

Explanation The registration with Cisco Smart Software Manager or satellite will expire soon.

Recommended Action Please initiate a registration renewal using 'Renew Registration Now' from the License Management web page or 'license smart renew ID' from the CLI. If a successful renewal is not done before the registration period expires, you will not be allowed to provision users or devices.

Error Message

%UC_SLMALARMCATALOG-4-SmartLicenseAuthorizationExpiringSoon: %[Reason=String] [AppID=String][ClusterID=String][NodeID=String]: The license authorization period will expire soon..

Explanation The license authorization period will expire soon.

Recommended Action Please initiate an authorization renewal using 'Renew Authorization Now' from the License Management web page or 'license smart renew auth' from the CLI before the authorization period expires.

Error Message

%UC_SLMALARMCATALOG-3-SmartLicenseRenewAuthFailed: %[Reason=String][AppID=String] [ClusterID=String][NodeID=String]: The license authorization renewal failed.

Explanation The license authorization renewal failed.

Recommended Action Please retry an authorization renewal using 'Renew Authorization Now' from the License Management web page or 'license smart renew auth' from the CLI. If the operation still fails, use RTMT to collect traces for Cisco Smart License Manager. Alternately, use CLI to collect traces by running the command file get activelog /cm/trace/slm/log4j/. If you are unable to resolve the issue contact TAC for assistance.

Error Message

%UC_SLMALARMCATALOG-3-SmartLicenseRenewRegistrationFailed: %[Reason=String] [AppID=String][ClusterID=String][NodeID=String]: The license registration renewal failed.

Explanation The license registration renewal failed.

Recommended Action Please retry a registration renewal using 'Renew Registration Now' from the License Management web page or 'license smart renew ID' from the CLI. If the operation still fails, use RTMT to collect traces for Cisco Smart License Manager. Alternately, use CLI to collect traces by running the command file get activelog /cm/trace/slm/log4j/. If you are unable to resolve the issue contact TAC for assistance.

Error Message

%UC_SLMALARMCATALOG-1-SmartLicenseExportControlNotAllowed: %[Reason=String] [AppID=String][ClusterID=String][NodeID=String]: This Unified Communications Manager is not licensed to operate in Mixed mode.

Explanation There are two requirements to run a Unified Communications Manager cluster in mixed mode. The cluster must run an export restricted version of software and an Encryption License must be available

Recommended Action PTo disable Mixed Mode run the CLI command â€˜utils CTL set-cluster non-secure-modeâ€™ on the Publisher. To continue running in Mixed Mode, this Unified CM Cluster must

be registered with Cisco Smart Software Manager or satellite with a token that allows Export-controlled functionality.

Error Message

%UC_SLMALARMCATALOG-4-SmartLicense_SLR_InEval: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: License Reservation is enabled on this system and the system is operating in Evaluation Mode that will expire soon.

Explanation License Reservation is enabled on this system and is pending Authorization Code installation for the reserved licenses.

Recommended Action Complete the license reservation process from CLI to avoid losing the ability to provision users and devices.

Error Message

%UC_SLMALARMCATALOG-2-SmartLicense_SLR_NoProvision_EvalExpired: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: License Reservation is enabled on this system and the license evaluation period has expired.

Explanation License Reservation is enabled on this system and is pending Authorization Code installation for the reserved licenses.The license evaluation period has expired.

Recommended Action Complete the license reservation process from the admin CLI in order to restore the ability to provision users and devices.

Error Message

%UC_SLMALARMCATALOG-1-SmartLicense_SLR_InOverage_NotAuthorized: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: License Reservation is enabled on this system. This system is operating with an insufficient number of licenses and the overage period is active.

Explanation License Reservation is enabled and the system is operating with an insufficient number of licenses.

Recommended Action Configure additional license in Smart Software Manager and redo the license reservation process from the admin CLI to avoid losing the ability to provision users and devices.

Error Message

%UC_SLMALARMCATALOG-2-SmartLicense_SLR_NoProvision_NotAuthorized: %[Reason=String][AppID=String][ClusterID=String][NodeID=String]: License Reservation is enabled on this system. This system is operating with an insufficient number of licenses and the overage period has expired.

Explanation License Reservation is enabled on this system. This system is operating with an insufficient number of licenses and the overage period has expired.

Recommended Action Configure additional licenses in Smart Software Manager and redo the license reservation process from CLI in order to restore the ability to provision users and devices.

Error Message

%UC_SLMALARMCATALOG-1-SmartLicense_SLR_ExportControlNotAllowed: %[Reason=String] [AppID=String][ClusterID=String][NodeID=String]: License reservation is enabled and this system is not licensed to operate in Mixed mode.

Explanation In order for this cluster to operate in Mixed Mode the cluster must be installed with a license reservation authorization Code from Smart Account and Virtual Account that allows Export-controlled functionality.

Recommended Action Disable Mixed Mode by running the CLI command ▒~@~Xutils CTL set-cluster non-secure-mode▒~@~Y on the Publisher. Otherwise to continue running in Mixed Mode, this Unified CM Cluster must be installed with a license reservation authorization Code from Smart Account and Virtual Account that allows Export-controlled functionality.

Error Message

%UC_HAPROXYALARMCATALOG-6-CiscoHAProxyServiceDown: %[AppID=String][ClusterID=String] [NodeID=String]: Service down

Explanation Service abruptly stopped

Recommended Action This problem occurs when an application is abruptly shut down or Service crashed.

Quick Links -

About Cisco

Contact Us

Careers

Connect with a partner

Resources and Legal -

Feedback

Help

Terms & Conditions

Privacy

Cookies / Do not sell or share my personal data

Accessibility

Trademarks

Supply Chain Transparency

Newsroom

Sitemap



© 2026 Cisco Systems, Inc.