



Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.6(2)

First Published: 2023-04-28

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 1994–2023 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface	xv
Change History	xv
About This Guide	xv
Audience	xvi
Related Documents	xvi
Communications, Services, and Additional Information	xvi
Field Notice	xvii
Documentation Feedback	xvii
Conventions	xvii

CHAPTER 1

Product Architecture	1
Cisco Unified Contact Center	1
Unified CM Peripheral Support and CTI OS	3
Router	3
Network Interface Controller	3
Logger	3
Peripheral Gateway	4
Open Peripheral Controller	6
Peripheral Interface Manager	6
Unified Communications Manager PIM	6
VRU PIM	6
Media Routing PIM	6
TDM ACD PIMs	7
JTAPI Gateway	7
CTI Gateway (CTI Server)	7
Configuration System	7

- Administration & Data Server 8
- Configuration Updates 8
- Reporting System 9
 - Historical Data Server 9
 - Unified Intelligence Center 10
 - Unified Intelligence Center Standard Deployment Model 10
 - Unified Intelligence Center Scaled Deployment Model 11
 - Unified Contact Center Management Portal 12
- Outbound Option 15

CHAPTER 2

Monitoring SNMP Health 17

- SNMP Overview 17
 - Faults 17
 - Instrumentation 19
- Base-Level SNMP MIB Support 19
 - SNMP Primary Agent 19
 - Base Level SNMP Subagents 19
 - Platform MIB Support 20
 - Host Resources MIB Subagent 20
 - MIB2 21
 - SYSAPPL MIB Subagent 21
- CISCO-CONTACT-CENTER-APPS-MIB 21
 - CISCO-CONTACT-CENTER-APPS-MIB Overview 22
 - CISCO-CONTACT-CENTER-APPS-MIB Structure 22
 - Mapping CCCA-MIB to Standard Host MIBs 24
 - CISCO-CONTACT-CENTER-APPS-MIB Objects 26
 - CCCA MIB Base Objects 27
 - CCCA MIB Instance Table Objects 27
 - CCCA MIB Component Table Objects 28
 - CCCA MIB Component Element Table Objects 29
 - CCCA MIB Router Table Objects 30
 - CCCA MIB NIC Table Objects 32
 - CCCA MIB Logger Table Objects 32
 - CCCA MIB Administration Server and Real-Time Data Server Table Objects 33

CCCA MIB Peripheral Gateway Table Objects	35
CCCA MIB Peripheral Interface Manager Table Objects	36
CCCA MIB CTI Gateway Table Objects	37
CCCA MIB CTI OS Table Objects	38
CCCA MIB Outbound Option Campaign Manager Table Objects	39
CCCA MIB Outbound Option Dialer Table Objects	40
Configuring the SNMP Agents	42
Installation Prerequisites for SNMP Support	42
SNMP Agent Configuration	43
Add Cisco SNMP Agent Management Snap-In	43
Save Snap-In View	43
Configure Community Names for SNMP v1 and v2c	44
Configure User Names for SNMP v3	45
Configure General Information Properties	47
Maximum Limits Settings for Agent Performance	49
Change Agent Log Quantity Setting	49
Configure SNMP Trap Destinations	49
Multihomed Windows Server	51

CHAPTER 3	Understanding SNMP Notifications	53
	Unified ICM/Unified CCE Notification Type	53
	cccaIcmEvent	53
	Dual State Objects	56
	Correlating Notifications	58
	Single State Objects	59
	Organizing SNMP Notifications	60
	CSFS Heartbeat Notification	60

CHAPTER 4	Syslog Message Interface	63
	The Cisco Log Message Format	63
	Configure Syslog Destinations	64

CHAPTER 5	Services and Processes	67
	Services	67

Using the Local Desktop 75
 ICM Service Control and Windows Task Manager 75
 Using the Local Registry 75
 Using the Remote SNMP Management Station 76

CHAPTER 6

Contact Center Trace Levels 79

Trace Levels 79
 Trace–All Nodes 80
 Trace–Administration and Data Server 80
 Trace–Router 81
 Trace–Logger 81
 Trace–Peripheral Gateway 82
 Trace–Web Setup 84
 Trace–Diagnostic Framework 84
 Trace–SADLib 85
 Reference Tables 85
 EMS Log Compression 86
 Dumplog 86
 EMS File Compression Control 87
 Other Registry Keys 87
 Set Router Tracing 87
 How to Set OPC Tracing 88
 General Diagnostics 89
 Diagnosing Network Transfer Issues 89
 Diagnosing Multimedia Issues 89
 Diagnosing VRU PG Issues 89
 How to Restore Default Trace Levels 90
 How to Display Trace Levels 90
 How to Set Unified CCM PIM Tracing 90
 How to Set JTAPI Gateway Tracing 90
 How to Set JTAPI Gateway Default Tracing 90
 How to Set Contact Sharing Tracing 91
 How to Set CTI Server Tracing 91
 Setting CTI Server Default Tracing 92

Setting CTI OS Tracing	92
Setting VRU PIM Tracing	92
Setting VRU PIM Default Tracing	93
Setting Outbound Option Tracing	93
How to Reset CampaignManager Tracing	93
How to Reset baImport Tracing	93
How to Reset Dialer Tracing	94
Trace File Retention Settings	94
Router Full Dump Enabled by Default	95

CHAPTER 7
Performance Counters 97

Import Unified CCE Data Collector Set Template	97
Platform Health Monitoring Counters	98
Platform Diagnostic Counters – Automatic Collection	101
Platform Diagnostic Counters	107
All Components	107
Logger/Administration & Data Server/HDS	108
SQL Server	109
Component-Specific Counters	109
Router	110
Logger	112
Administration & Data Server	113
PG – OPC	114
PG – Communications Manager (EA) PIM	116
PG – VRU PIM	117
CTI Server	118
CTI OS Server	120
Outbound Option Campaign Manager	123
Outbound Option Import	124
Outbound Option Dialer	124
Message Delivery Service	126
QoS	136

CHAPTER 8
Capacity Planning 141

Capacity Planning Process	141
Capacity Planning – Getting Started	142
Finding the Busy Hour	142
Collected Data Categorization	143
Current Deployment Design	143
Configuration Information	144
Traffic Load	145
Migration Requirements	145
Platform Performance	146
Capacity Utilization	146
CPU Utilization Calculations	147
Memory Utilization Calculations	147
Disk Utilization Calculations	148
NIC Utilization Calculations	148
Maximum Utilization Calculations	148
Relating Traffic Load to Resources	148
<hr/>	
CHAPTER 9	Diagnostic Tools 151
Diagnostic Framework	151
Overview	151
Installation and Configuration	151
Service Registration and Dependencies	152
Configure Service Port	152
Enabling ECDSA	153
Installing or Updating Third-Party Certificate	154
Diagnostic Framework Log Files and Logging Level	154
Diagnostic Framework Service Resources Requirements	154
Security	155
Log In to the Diagnostic Framework Portico	156
Authentication, Authorization, and Auditing	156
Encryption	159
Certificate Management	159
Usage	161
Accessing the Diagnostic Framework Through the Analysis Manager	162

Accessing the Diagnostic Framework Through the Unified System CLI	162
Accessing the Diagnostic Framework Through the Built-In User Interface (Portico)	188
Accessing Diagnostic Framework Commands Through a Browser	188
CLI Configuration	189
Deployment Option 1: CVP OAMP	189
Configure System CLI with CVP OAMP	189
Modify or Add User to CVP OAMP for System CLI	191
Install CVP Remote Operations	191
Add Remote Operations Machines to CVP Operations Console	192
Confirm Windows Environment Variables Set Correctly for CVP Web Services	193
Use Unified System CLI with CVP OAMP	193
Deployment Option 2: Devices.csv	194
Create Devices.csv from Sample File	194
Add Connection Information to Devices.csv File	195
Designate Users for Diagnostic Framework	196
Use Unified System CLI with Devices.csv	197
Running the System CLI from Multiple Machines with Devices.csv	198
Diagnostic Framework API	198
GetTraceLevel	198
SetTraceLevel	199
ListTraceComponents	199
ListTraceFiles	201
DownloadTraceFile	201
ListLogComponents	202
ListLogFiles	203
DownloadLogFile	203
ListAppServers	204
ListConfigurationCategories	204
GetConfigurationCategory	205
GetProductVersion	205
GetProductLicense	205
GetNetStat	206
GetIPConfig	206
GetTraceRoute	206

- GetPing 206
- ListProcesses 206
- ListServices 207
- GetPerformanceInformation 208
- GetPerfCounterValue 208
- GetAlarms 209
- SetAlarms 211
- SNMP/Syslog REST API 211
 - General Information 212
 - SNMP v1/v2c Community 215
 - SNMPv3 User 221
 - Traps 229
 - Syslog 235
 - Update Implementation for SNMP/Syslog REST APIs 239
- Diagnostic Framework Troubleshooting 240
- DUMPLOG 241
- EMSMON 245
 - How to Run EMSMON 246
 - Monitoring Process 246
 - Run EMSMON Remotely 246
 - EMSMON Connections 246
- Unified CCE Certificate Monitoring Service 247
 - Certificate Monitoring Events 247
 - Certificate and Key Validation 248
 - Serviceability 249
 - Supported Log Levels 249
 - Configuration Parameters 249

CHAPTER 10

Serviceability for VOS-Based Contact Center Applications 251

- VOS-Based Contact Center Applications 251
- Real Time Monitoring Tool 251
 - Install and Launch RTMT 252
 - RTMT Client Support Services 253
 - The RTMT Interface 253

Download Trace and Log Files	254
View the Status of Services	256
Alert Central	257
Cisco Identity Service Alerts	258
Cloud Connect Syslog and Alert	259
View Performance Counters	260
Disaster Recovery	260

CHAPTER 11

Cloud Connect Serviceability	261
Cloud Connect Platform	261
Collect service logs using RTMT	261
View Real-time service logs using RTMT	262
Purge log files using CLIs	263
Serviceability for Web Proxy	263
Set up trace levels	263
Collect Web Proxy logs	263
Serviceability for Cloud Connect Management	264
Set up trace levels	264
Download Cloud Connect Management logs	264
View the status of Cloud Connect Management service	265
Serviceability for Digital Routing	266
Configure Service Logging	266
Configure service logging using API	266
Configure service logging using CLI	268
Configure syslog	269
Configure syslog using API	269
Configure syslog using CLI	270
Monitor the status of the Digital Routing service	270
Download logs using CLI	271
Directory listing	272
Access JMX counters	272
Access JMX Counters using API	272
Access Counters using JConsole	276
Access Digital Channel Statistics in CCE Administration Portal	277

JMX Service counter definitions	277
Serviceability for DataConn	283
Download DataConn logs	283
Monitor the status of DataConn service	283

CHAPTER 12
Live Data Serviceability 285

Live Data Reporting System	285
Live Data Collecting Logs	285
Live Data Log Levels	286
Set Live-Data Trace Agent	287
Set Live-Data Trace Skill-Group	289
Set Live-Data Trace Precision-Queue	290
Live Data Failover Configuration	291
set live-data failover	291
unset live-data failover	291
show live-data failover	292
Live Data Syslog	293
set live-data syslog-server	293
unset live-data syslog-server	293
show live-data syslog-server	294
Monitor and Analyze System Performance Using Nmon	294
utils live-data nmon start	294
utils live-data nmon stop	294
Live Data Socket.IO	295
show socketio status	295
Live Data SNMP	296
Live Data CISCO-LIVEDATA-MIB	296
Live Data MIB Textual Conventions	297
Live Data MIB General Objects	298
Live Data MIB Cluster Information	298
Live Data Service Table	299
Live Data Reporting Connection Table	300
Live Data Event Table	301
Live Data MIB Notifications	303

	Live Data SNMP Event Correlation	303
	Live Data SNMP Parameters	304
<hr/>		
CHAPTER 13	Cisco Identity Service Serviceability	307
	Cisco Identity Service Logs	307
	Set the Cisco Identity Service Log Levels	307
	Set up a Remote Syslog Server	308
<hr/>		
CHAPTER 14	CCE Serviceability and Monitoring using AppDynamics	309
	Overview	309
	Supported Applications	309
	Prerequisites	311
	Application Group and Agent Licenses	311
	Cloud Connect	311
	CCE Solution Components	312
	Performance Monitoring	312
	Enable Performance Monitoring	313
	Update Performance Monitoring Configuration	317
	Disable Performance Monitoring	317
	Check Status of Performance Monitoring	318
	Test Connection with AppDynamics Controller	318
	Configure Thresholds and Alerts for Monitoring	318
	Configure JMX Monitoring and Alerting Templates for Finesse Desktop	319
	Dashboards	319
	Create Dashboards Using Templates	320
	End User Monitoring	320
	View Metrics	321
	Check Logs	323
	Things to Know	325
<hr/>		
APPENDIX A	MIB Results Example Appendix	327
	Cisco Contact Center Applications MIB Results Example	327
<hr/>		
APPENDIX B	Unified ICM/Unified CCE SNMP Notifications	331

Administrative Data Server SNMP Notifications 332

Node Manager SNMP Notifications 332

Message Delivery Service SNMP Notifications 340

Router SNMP Notifications 343

Logger SNMP Notifications 353

Peripheral Gateway SNMP Notifications 361

CTI SNMP Notifications 367

Live Data Events 376

Live Data TIP Server SNMP Notifications 393

Outbound Option SNMP Notifications 398

ICM Network Interface Controller SNMP Notifications 410

TDM Peripheral Gateway SNMP Notifications 449



Preface

- [Change History](#), on page xv
- [About This Guide](#), on page xv
- [Audience](#), on page xvi
- [Related Documents](#), on page xvi
- [Communications, Services, and Additional Information](#), on page xvi
- [Field Notice](#), on page xvii
- [Documentation Feedback](#), on page xvii
- [Conventions](#), on page xvii

Change History

This table lists the changes made to this guide. The most recent changes appear at the top.

Change	See	Date
Initial Release of Document for Release 12.6(2)		April 2023
Added new sections for Serviceability of Cloud Connect Platform and docker services.	Cloud Connect Serviceability	27 February 2023
Changes related to merging proxy CLI for app monitoring with enable and status CLIs.	Enable Performance Monitoring and Update Performance Monitoring Configuration sections.	01 Feb 2023
Added a statement for the use of HTTPS.	Accessing the Diagnostic Framework Through the Built-In User Interface (Portico).	28 November 2022

About This Guide

This document contains system diagrams, staging steps and sample test cases for supported models of Unified ICM/CCE.

The supported models are:

- Dedicated Forest/Domain Model
- Child Domain Model
- Hosted Network Applications Manager (NAM) / Customer ICM (CICM) Model



Note This document is for individuals responsible for staging deployments of Cisco contact centers. Individuals must be trained on the use and functions of Unified ICM/CCE & Hosted as well as Microsoft Windows Server, Active Directory (AD), and DNS. This document does not provide detailed Cisco Unified Intelligent Contact Management Enterprise (Unified ICM), Hosted NAM/CICM, or Microsoft Windows Server specific information. You can find this information elsewhere in specific documentation from Cisco or Microsoft.

Audience

Individuals utilizing this document must have knowledge and experience with the following tools/software/hardware to stage the system software as described in this document:

- Cisco Unified ICM Scripting and Configuration Tools
- Third-party software (if installed)
- Microsoft Windows Server and Windows Active Directory administration
- Microsoft SQL Server administration

Related Documents

Document or Resource	Link
Cisco Unified Communications Manager	https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/tsd-products-support-series-home.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).

- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround, or other user action. For more information, see *Product Field Notice Summary* at <https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html>.

You can create custom subscriptions for Cisco products, series, or software to receive email alerts or consume RSS feeds when new announcements are released for the following notices:

- Cisco Security Advisories
- Field Notices
- End-of-Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

For more information on creating custom subscriptions, see *My Notifications* at <https://cway.cisco.com/mynotifications>.

Documentation Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	<p>Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names.</p> <p>For example:</p> <ul style="list-style-type: none"> • Choose Edit > Find. • Click Finish.

Convention	Description
<i>italic font</i>	Italic font is used to indicate the following: <ul style="list-style-type: none">• To introduce a new term. Example: A <i>skill group</i> is a collection of agents who share similar skills.• A syntax value that the user must replace. Example: IF (<i>condition, true-value, false-value</i>)• A book title. Example: See the <i>Cisco Unified Contact Center Enterprise Installation and Upgrade Guide</i>.
window font	Window font, such as Courier, is used for the following: <ul style="list-style-type: none">• Text as it appears in code or that the window displays. Example: <code><html><title>Cisco Systems, Inc. </title></html></code>
< >	Angle brackets are used to indicate the following: <ul style="list-style-type: none">• For arguments where the context does not allow italic, such as ASCII output.• A character string that the user enters but that does not appear on the window such as a password.



CHAPTER 1

Product Architecture

- [Cisco Unified Contact Center, on page 1](#)
- [Router, on page 3](#)
- [Logger, on page 3](#)
- [Peripheral Gateway, on page 4](#)
- [Configuration System, on page 7](#)
- [Reporting System, on page 9](#)
- [Outbound Option, on page 15](#)

Cisco Unified Contact Center

Unified CCE delivers intelligent contact routing, call treatment, network-to-desktop computer telephony integration (CTI), and multichannel contact management over an IP infrastructure. It combines multichannel automatic call distributor (ACD) functionality with IP telephony in a unified solution, enabling you to rapidly deploy a distributed contact center infrastructure.

Unified CCE provides the following services:

- Segmentation of customers and monitoring of resource availability
- Delivery of each contact to the most appropriate resource anywhere in the enterprise
- Comprehensive customer profiles using contact-related data, such as dialed number and calling line ID
- Routing to the most appropriate resource to meet caller needs based on real-time conditions (such as agent skills, availability, and queue lengths)

Unified CCE enables you to smoothly integrate inbound and outbound voice applications with internet applications such as real-time chat, web collaboration, and email. This integration enables a single agent to support multiple interactions simultaneously regardless of which communications channel the customer chooses.

Unified CCE is a distributed solution with no single-server implementation. Unified CCE employs multiple servers each with multiple software components. Deployment options are flexible with performance, capacity, and network topology driving the deployment design.

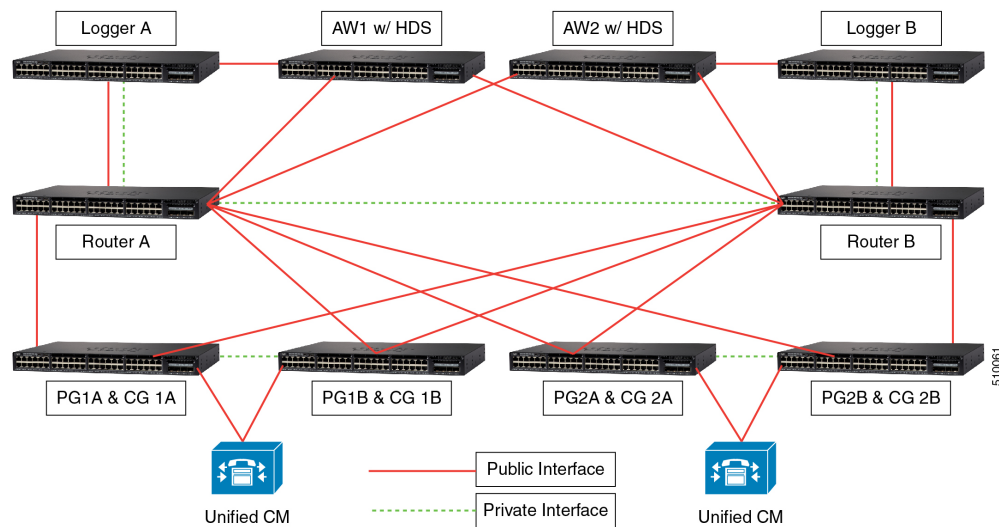
Unified CCE was derived from Unified ICME with the primary difference being that Unified CCE integrates only with the Cisco Unified Communications Manager (Unified CM) IP PBX. All other major components of the Unified CCE solution are the same as the Unified ICM solution.

The Unified ICM platform is designed to route calls between various nodes in the TDM phone network. It is designed with an emphasis on reliability and flexibility. All processing in these components is message-based. The content of the message and the current state of the process determines the processing of each message. The messages are delivered to these components using the Unified ICM Message Delivery Service (MDS). MDS ensures that both processes are fed the exact same set of messages in the same order.

One of the most important concepts to understand about Unified CCE is its redundancy strategy. The components that contain centralized state are run in duplex. Two of these components work in lockstep to ensure redundancy and immediate recovery from a fault.

From a device standpoint, a typical Unified CCE deployment looks as follows:

Figure 1: Unified CCE Architecture



There are four major components of a Unified CCE deployment: the Router, the Logger, the Peripheral Gateway (PG), and the Administration & Data Server. The basic function of each is as follows:

- **Router**—Make the routing decisions. The router selects a peripheral or agent to receive an inbound contact (voice call, email, chat, and so on).
- **Logger**—Store (and replicate) all configuration, real-time and historical data.
- **Peripheral Gateway**—Act as a gateway to a peripheral device, like an IP PBX or a Voice Response Unit (VRU), and a CTI gateway linking agent desktops.
- **Administration & Data Server**—A server implementation that provides configuration data (from the Logger), an interface for real-time data, and a platform for the historical data server (HDS). The Administration & Data Server also offers an interface for administrators to alter configuration and routing scripts (Script Editor, Internet Script Editor).



Note Unified CCE applications do not report their resource usage to monitoring solutions, like Cisco Prime Collaboration. The monitoring solution retrieves CPU and memory usage data directly from the Windows Server operating system. On multicore systems, Windows Server might report usage greater than 100% while the Unified CCE solution is running as usual.

Unified CM Peripheral Support and CTI OS

Cisco Finesse replaces CTI OS for Unified CCE.

CTI OS is no longer supported with Unified CCE. However, CTI OS is supported with UCCE System PG and other TDM peripheral types.

The CTI OS server setup now has the option to select UCCE System instead of UCCE. The setup also validates whether the selected peripheral is configured, through the Peripheral Gateway Setup, as UCCE System peripheral or not.

Router

The Router is the brain of Unified CCE. Unified CCE can run user-defined scripts to make decisions on what happens with calls, and can determine how to get a call from one place to another. The Router communicates with several other components, including the Logger, the PGs, and the Administration & Data Servers (ADSs).

The Router receives notification from routing clients (PGs) that a call is in need of some form of routing. It then runs a user-defined script to determine what to tell the routing client to do with the call.

In addition, the Router receives status events and reporting events from PGs. The Router uses these messages to update its current representation of the agents and resources in the system, which is used by the scripts to determine where to send calls. It also sends these messages to the Logger for storage and some of the messages to the Admin Workstations for real-time reporting.

Routers, Loggers and PGs are fault tolerant, having two instances of each component so that a failure of one provides for bump-less continuation of function through the remaining half of a duplex pair. Routers are duplex entities, which means that two separate, distributed instances (identified as Side A and Side B) use the MDS to keep in lockstep with the other side, ensuring that any outage of one side guarantees that the system continues operating without failures or impairments—the opposite side assuming sole responsibility for making routing decisions. All data as well as call control messaging is shared between sides to ensure that both sides have the same data by which to make (the same) routing decisions. Both Router sides are concurrently in service.

Network Interface Controller

Like a PG, a Network Interface Controller (NIC) is a type of routing client. However, a NIC is more limited than a PG. A NIC is used to interact with a telephony network, usually the TDM. A NIC is typically coresident with the Router and used for Unified ICM deployments.

Logger

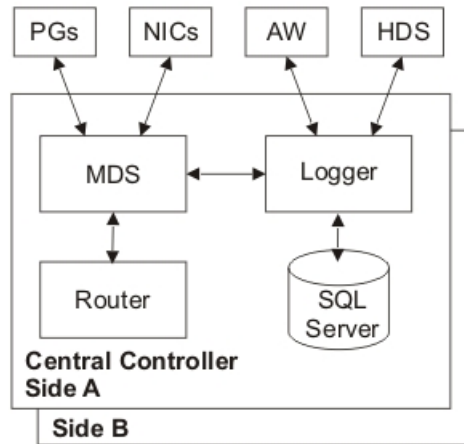
Unified CCE uses the Logger to store historical data and configuration data about the call center. The Logger is the place where historical data is first stored, and from which it is later distributed. The Logger receives messages from the Router. These messages include detail messages about the calls and summary messages that the PGs compute and send through the Router. Examples of these summary messages are half-hour summaries (how many calls were received during a given period).

The Logger uses a synchronization process that is a little different than the Router. The messages coming to the Logger are sent only from the corresponding Router. Side A Router sends messages only to the Side A Logger. Side B Router sends messages only to the Side B Logger. Because the Routers are running in lockstep,

it is guaranteed that while messages are flowing they are the same messages. However, recovery happens directly from Logger to Logger, using bulk database copy algorithms for efficiency.

The Loggers also distribute historical data to HDS and configuration and real-time data to the Administration & Data Servers through MDS. Loggers are duplex as well and are tightly coupled with their respective Router. In many deployments, a side of the Router and Logger are collocated on the same physical server. A Router/Logger combination is often referred to as the Central Controller.

Figure 2: Central Controller Architecture



Peripheral Gateway

The PG is the component that talks to the telephony devices through their own proprietary CTI interface in a Unified CCE system. These devices can be ACDs, IVR devices or, in cases such as with Unified CCE, an IP PBX. The PG normalizes whatever protocol the telephony device speaks, and keeps track of the state of agents and calls that are on that device. The PG sends this status to the Router, as well as forwards requests requiring customer logic to the Router.

The PG also exposes a normalized CTI interface to clients. These clients can be traditional CTI clients (wallboards, agent/supervisor desktop clients, and so on), or they can be another instance of Unified CCE, as is the case in a parent/child deployment.

The component of the PG that does the normalization is called a Peripheral Interface Manager (PIM). This component talks to the peripheral and translates whatever proprietary language it speaks into the normalized one that the Open Peripheral Controller (OPC) and the rest of the PG understand.

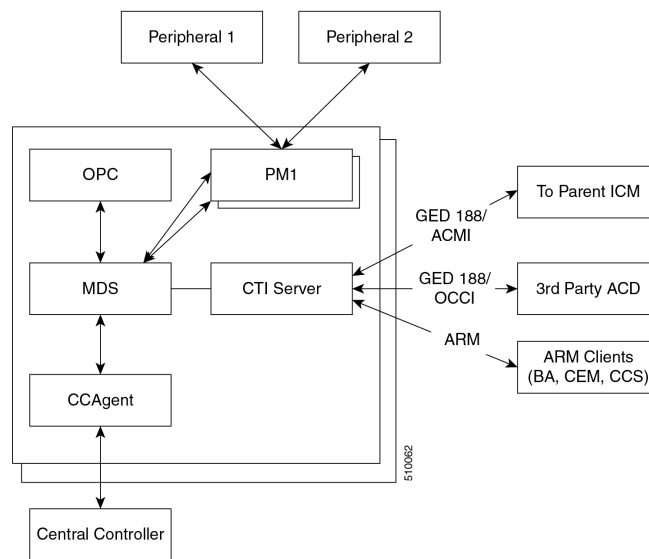
PGs fall into several groups. The first classification of PG includes those that talk to an ACD or Unified CM that has agents on it. This is the typical case for a PG. It talks a proprietary CTI protocol to the switch, and maintains the state of agents and calls in queue on the device. While all of these PGs report agent state to the Central Controller, they do it in a different way. In the case of a PG talking to an ACD, the PG mirrors the state of the agents on the ACD; it keeps a copy of the primary state of the agents tracked by the ACD. In the case of a PG attached to a Unified CM, the Unified CM does not know about agents or agent states, it only knows about phone lines. In this case the PG is the primary for the agent state.

The second classification of PG is a VRU or Media Routing (MR) PG. These PGs expose an interface that is client-neutral. In the case of the VRU PG, this interface is tailored to voice calls; in the case of the MR PG,

it is more generic task routing that is exposed. These PGs do not maintain agent state, but only maintain the state of calls (or tasks) and expose an interface for the devices to get instructions from the Router.

The third classification of PG is the group PG. There are two types of PGs that talk to groups of peripherals. The first is the Generic PG. This PG allows multiple PIMs of different types to reside inside of the same PG. Each peripheral on this PG behaves completely independently. Currently the Generic PG is supported only for Unified CCE, where it contains a Communications Manager PIM and a VRU PIM talking to an IP-IVR or Customer Voice Portal (CVP). The second type of group PG is a Unified CCE System PG. This PG, like the generic PG, has one Call Manager PIM and one or more VRU PIMs. The System PG ties these multiple PIMs together. In a traditional Unified CCE, a call that comes into the Communications Manager then gets transferred to the IP-IVR and then back to an agent looks like three separate calls to Unified CCE. The System PG coordinates these calls and makes that call look like a single call. This is what happens on a traditional TDM ACD, where the ACD also has a queue point.

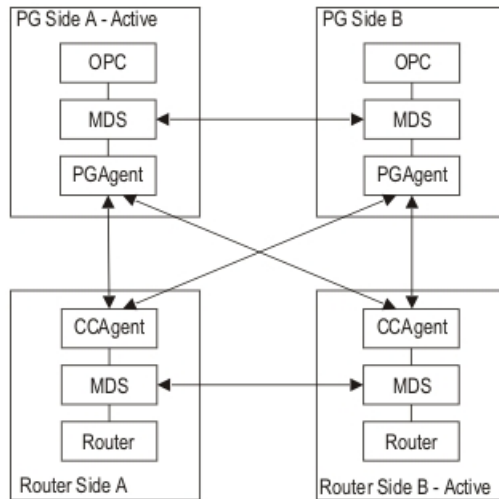
Figure 3: Peripheral Gateway Architecture



The PG is duplexed using the same technology as the Central Controller, MDS. This means that there are two PGs operating at any time. All of the messages to the critical process on the PG (OPC) go through the MDS queue, to keep the two operating in lock-step. However, the PG operates slightly different from the Router – from a fault tolerance standpoint – in that while both sides share the same data, for many PG components, only one side is active. Should a fault occur, the opposite side activates and continues functioning, having the context of the other side without losing calls.

PGs use the Device Management Protocol (DMP) to communicate between themselves and the central controller. The following figure depicts the components involved in this communication and the communication links employed.

Figure 4: DMP Flows



Coresident with the PG is the CTI Gateway (CG - CTI Server component).

Open Peripheral Controller

The Open Peripheral Controller (OPC) computes and maintains the state of agents on the PG. The OPC reports that state to the Router, knows when a call requests instructions from the Router, and performs the CTI operations on the telephony device as necessary. OPC is the critical process on the PG. It is kept in lock-step with its sibling on the other side.

Peripheral Interface Manager

The Peripheral Interface Manager (PIM) is responsible for the connection to the peripheral (ACD, PBX, IVR). This process is not a lock-step process nor is data shared between the two sides. Instead either the Side A or Side B PIM is active for each peripheral. If one side loses its connection, the other side activates.

Unified Communications Manager PIM

Unified CCE Only

The Communications Manager PIM provides the interface between the Unified CM and the Unified CCE OPC process. This PIM communicates with Unified CM through the JTAPI Gateway.

VRU PIM

The VRU PIM provides an interface to a VRU (or IVR). The communication protocol used between the PIM and the VRU is GED-125.

Media Routing PIM

The Media Routing (MR) PIM provides the integration point for multimedia contacts such as emails or collaboration (chat) sessions. It is also a necessary component for integration of the Outbound Option Dialer.

TDM ACD PIMs

The TDM ACD PIMs provide interfaces to various manufacturers' Automatic Call Distributors. The communication protocol between the PIM and the ACD is typically proprietary.

JTAPI Gateway

Unified CCE only

The JTAPI Gateway is a process that connects to the Unified CM CTI Manager and provides the link between the peripheral gateway and the Unified CM cluster. The Unified CM CTI Manager communicates CTI messages to and from other nodes in the Unified CM cluster. The JTAPI Gateway provides an added level of translation between the (Java) JTAPI interface and the (C++) Unified Communications Manager PIM.

CTI Gateway (CTI Server)

The CTI Server is the interface from OPC to CTI clients. It provides an interface (protocol) specified as GED-188. This interface has many variances and message sets. It was used as a direct CTI connection to agent desktops or third-party desktops. This use is deprecated.

GED-188 helps to hide the details of individual peripherals, but does not fully complete the job. The messages sent from a CTI Server connected to an Aspect PG differ from the messages sent from a CTI Server connected to a Unified CCE PG.

Today the CTI Server connects to several types of clients:

- Agent Reporting and Monitoring (ARM) clients – this variance of GED-188 allows reporting agent status and receiving information about the status of agents. It is one of the integration points for multichannel (email and web collaboration) applications and for the Outbound Dialing options.
- Parent ICM – a single connection is allowed to a CTI Server attached to a Unified CCE System PG. This connection allows the parent ICM to receive status about agents and calls on this PG, and to take control of certain incoming calls and route them itself. This variance of GED-188 is known as ACMI.

At any given time, only Side A or Side B CTI Server is active, not both. Clients must connect to one or the other.

Configuration System

The Unified CCE configuration system is also based around the concept of reliability and scalability. There can be multiple configuration database copies, which are kept in sync using MDS and a synchronization process from the central controller. Each of these can send updates to the Router, but only the Logger configuration database is authoritative.

The configuration system consists of the DBAgent process on the Router, which accepts connections from the Administration & Data Servers, and distributes configuration updates to those Administration & Data Servers. The Administration & Data Servers have a copy of the configuration and expose a GUI for browsing and making changes. The Administration & Data Servers also expose an API (ConAPI) for accessing the configuration information and for making changes.

Administration & Data Server

The Administration & Data Server is the main interface to the Unified ICM/Unified CCE configuration. On the Administration & Data Server resides a database that contains a copy of the configuration information in the Logger. A Distributor process, which receives updates from the central controller, writes to the database to keep everything in sync. Multiple clients read the configuration from the database and send update messages to the central controller DBAgent process.

The two main clients in the Administration & Data Server are the configuration tools, and the Configuration Management Server (CMS) process. The configuration tools are used to provide a GUI to update the configuration. The CMS process is used to provide the Configuration API (ConAPI).

Processes that connect to ConAPI are the multichannel components for agent and skill group management and CCMP.

The Administration & Data Server does not have a dependent twin, but rather provides fault tolerance in numbers (N+1 model). A typical Unified ICM/Unified CCE deployment often has two or more Administration & Data Servers. Administration & Data Servers connect to each central controller side – a primary and a secondary. If a failure occurs on the primary link, the secondary recovers from the failure and restores connectivity.

Configuration data is supported on multiple Administration & Data Server types:

- Administration Server and Real-time Data Server (AW Distributor) (with no HDS; configuration and real-time data but no historical or call detail data)
- Administration Server, Real-time and Historical Data Server, and Detail Data Server (AW-HDS-DDS), (configuration, real-time, historical, and call detail data)
- Administration Server and Real-time and Historical Data Server (AW-HDS) (configuration, real-time and historical data but no call detail data)
- Administration & Data Server configuration (AW-CONFIG, configuration data only)

Configuration changes are not supported on the HDS-DDS type (which includes historical and call detail data but excludes real-time data). The HDS-DDS type includes only configuration data needed for historical reporting purposes.

Configuration Updates

Figure 5: Configuration System Message Flow

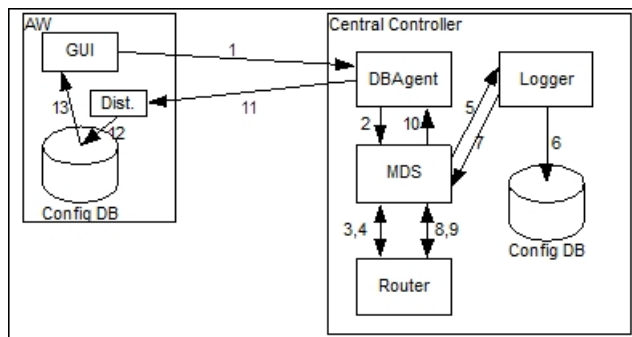


Figure 5 illustrates how a configuration update may happen in Unified CCE:

- In the first step (not shown) an Administration Client reads configuration from the database, and determines that a change is required.

- When this determination happens, the GUI connects to the DBAgent process on the central controller and sends the update (Step 1).
- DBAgent sends the message to the Router, through MDS (Steps 2, 3).
- The Router validates the configuration message and sends it to the Logger to be run (Steps 4, 5).
- The Logger updates its configuration (Step 6).
- The Logger sends confirmation of the update to the Router (Steps 7, 8).
- The Router then sends the update to all its clients (DBAgent, PGs, and so on) (Step 9, 10).
- DBAgent sends this message to each of its Administration Server and Real-time Data Servers (Step 11). The Administration Server and Real-time Data Servers update their database (Step 12).
- The Configuration GUI detects the change happen (Step 13).

Reporting System

The reporting system for Unified ICM/Unified CCE is similar to its configuration system; they use the same distribution channel:

Reporting messages are generated by PGs (this includes both detail messages and summary messages) and then are sent to the Central Controller, which consists of the Router and the Logger.

The Router feeds real-time data to the Administration Server and Real-time Data Servers.

The Logger stores historical data and replicates it to the Historical Database.

Administration Server and Real-time Data Servers write those records into the real-time reporting database. Those Administration Server and Real-time Data Servers that are configured to have Historical Data Servers also write the appropriate records to the historical database. Cisco Unified Intelligence Suite (Unified IS) are web applications that uses Java Servlets to build reports to be viewed from thin (web browser) clients.

Historical Data Server

The Historical Data Server (HDS) is an option to be installed with an Administration Server and Real-time Data Server. It uses the same distributor technology used to keep the configuration database up to date. The HDS provides a long-term repository for historical data and offloads historical reporting from the Logger. Historical data is replicated from the Logger to one or more HDSs.

There are three types of HDSs:

- **Administration Server, Real-time and Historical Data Server, and Detail Data Server (AW-HDS-DDS):** HDS with call detail data store. This type includes both real-time and configuration data and you can use it to source historical data for the Analysis Call Path tool. This type is intended for small- to medium-sized deployments. There may be a maximum of two AW-HDS-DDS servers per Logger side in small or medium deployments but only one per Logger side in a large deployment (presumably with multiple AW-HDS servers).
- **Administration Server and Real-time and Historical Data Server (AW-HDS):** HDS without a call detail data store (no call detail, call variable, agent state data). This type also includes both real-time and configuration data but you cannot use it to source data for the Analysis Call Path tool. This type is intended for large deployments. There may be a maximum of three AW-HDS per Logger side.
- **HDS-DDS:** HDS with call detail data store but no real-time data or configuration data. This type may be used to source historical data for the Analysis Call Path tool. This type is intended for large deployments and for use with multiple AW-HDS servers. There may be a maximum of one HDS-DDS per Logger side (presumably with multiple AW-HDS servers).

Unified Intelligence Center

Unified Intelligence Center is a web-based reporting platform for the Cisco Unified Communications products and is supported by Unified ICME and Unified CCE.

You can install Unified Intelligence Center as a standalone server or in a cluster of a maximum of eight server nodes. There is one mandatory publisher node (called the Controller) and up to seven subscriber nodes (called Members). The Controller node includes a Member, which means a deployment can consist of a Controller only.

Cisco Unified Intelligence Center offers both a web-based reporting application and an administration interface. The reporting application runs on the Members. The administration application runs on the Controller.

Unified Intelligence Center reporting features include multi-user support, customized reports, security, multiple display formats, web accessibility, and Web 2.0-like mashup support to display data from multiple sources on a single dashboard. These features make Unified Intelligence Center a valuable tool in the information technology arsenal of any organization and position it as a drop-in replacement or solution for most reporting requirements.

Cisco Unified Intelligence Center reporting capabilities include:

- Web 2.0 based dashboard mashups
- Powerful grid presentations of reports with sorting and grouping
- Chart and gauge presentations of reports
- Association of multiple report displays with the same report definition
- Custom filters
- Custom thresholds to alert on the data
- Pre-installed stock report templates for Unified CCE data
- Ability to report data from JDBC compatible data sources

Unified Intelligence Center supports the following:

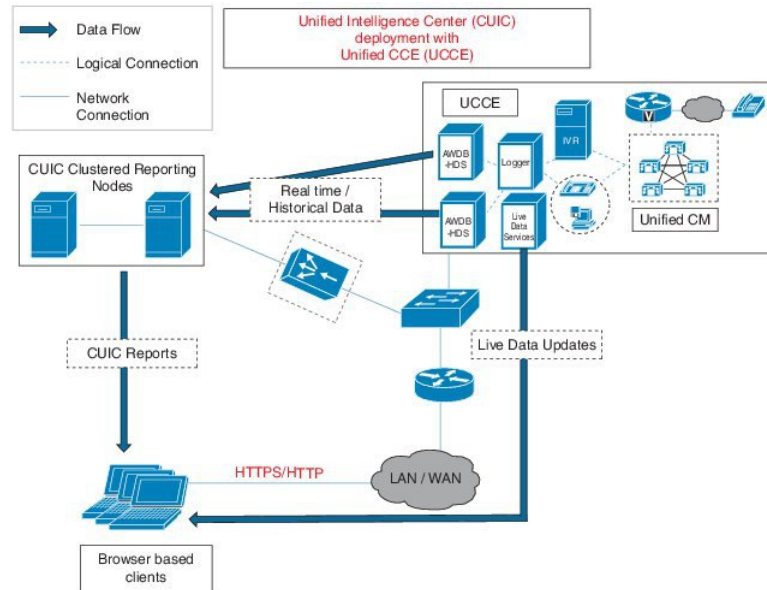
- Multiple users
- Customized dashboards and custom reports
- Report scheduler
- Detailed security levels and LDAP/local database authentication
- Import and export of report XML files
- Export of grid reports to Microsoft Excel
- Multiple languages
- Clustered deployment
- Management support through Simple Network Management Protocol (SNMP), Java Management Extensions (JMX), and Cisco Analysis Manager

Unified Intelligence Center Standard Deployment Model

The Unified Intelligence Center deployment with Unified CCE uses the AW-HDS as its data source server. You can connect to multiple AW-HDS databases to handle the load from multiple Unified Intelligence Center reporting nodes. You can use other data sources, such as the CVP Reporting Server, along with the Unified CCE AW-HDS as data source servers. The ACE load balancer, an optional component, provides load balancing for report queries across the multiple reporting nodes and servers as a single point of access to the cluster.

You can use Unified CCE deployments with a distributed AW-HDS as a data source for Unified Intelligence Center reports. However, local area network AW-HDS access ensures enhanced throughput in data extracted and ensures faster response times for reports, especially real-time reports with repeated refresh intervals.

Figure 6: Unified Intelligence Center Standard Deployment



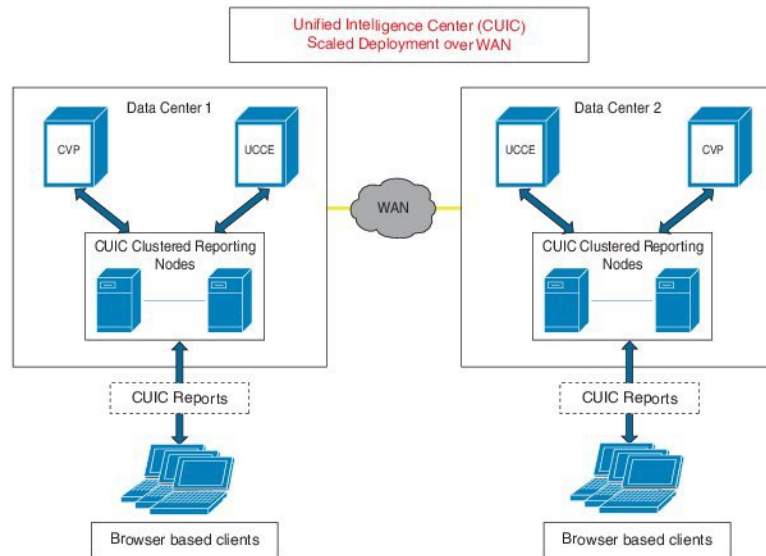
303007

Unified Intelligence Center Scaled Deployment Model

You can deploy Unified Intelligence Center as the reporting solution with Unified CCE deployments that scale over WAN networks. In these deployments, Unified Intelligence Center is deployed locally with one section or data center of the scaled Unified CCE deployment. Unified Intelligence Center can access the local AW-HDS over the Local Area Network (LAN), and the remote AW-HDS, which is deployed along with the remote section of Unified CCE over the Wide Area Network (WAN).

You can deploy other data sources, such as the Cisco Unified Customer Voice Portal, along with Unified CCE. Firewall considerations when you deploy over the WAN apply to the data source servers. Open appropriate ports as described in *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/en/US/products/sw/custcosw/ps1844/tsd_products_support_series_home.html, depending on the remote database configuration.

Figure 7: CUIC Scaled Deployment



Unified Contact Center Management Portal

Unified CCMP is a suite of server components that simplify the operations and procedures for performing basic administrative functions such as managing agents and equipment, and provide a common, web-based user interface within the entire Unified CCE product set. Unified CCMP consists of four components:

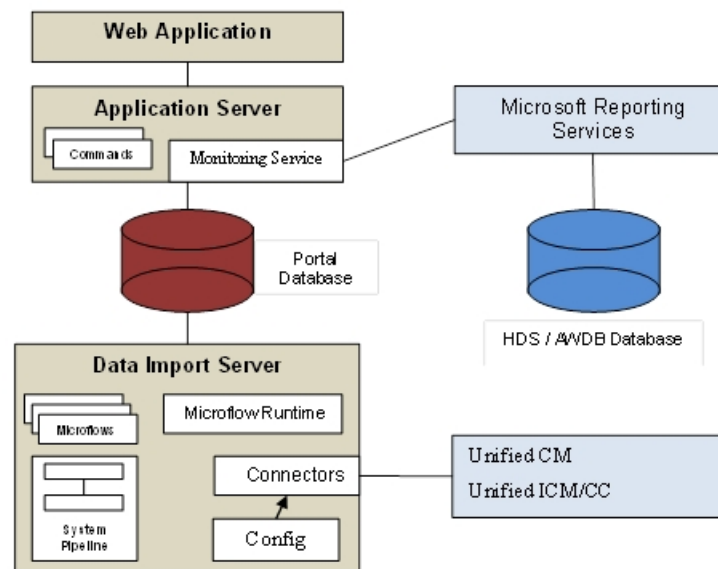
- The Database Server component, which uses an application called the Importer to import enterprise data from different data sources into a Microsoft SQL Server management information database. The database consists of separate database elements that sit on top of the SQL Server and that provide data to different reporting elements:
 - RDBMS Database (known as the datamart) holds the imported enterprise data.
 - Reporting Services Database imports and processes data from the datamart so that SQL Server Reporting Services can use it to populate reports.
- The Application Server component manages security and failover. It manages security by ensuring that users can view only specific folders and folder content as defined by their security sign-in credentials. It verifies that a user is valid and then loads the system configuration that applies to that user. It also manages failover. So if one database server fails, the application can automatically retrieve the required data via an alternative database server.
- The Web Server component provides a user interface to the platform. The user interface allows users to work with report data, and perform administrative functions.
- The Data Import Server component is an Extract, Transform, and Load (ETL) server for data warehouses. The Data Import component imports the data used to build reports. It is designed to handle high volume data (facts) such as call detail records and data that is rarely changed (dimensions) such as agents, peripherals, and skill groups.

If you install these components on more than one server, you generally install the Data Import and Database components on the Database Server. You usually install the Application and Web components on the Web Application Server.

Unified CCMP maintains a complete data model of the contact center equipment to which it is connected and periodically synchronized. In addition to configuration information such as agents or skill groups, the Unified CCMP can optionally record the events logged by the equipment. These records are used for management information and reporting purposes. Unified CCMP data model and synchronization activity allows for items to be provisioned either through the Unified CCMP Web interface or from the standard equipment specific user interfaces.

The following illustration shows the Unified CCMP system architecture. The top half of the diagram is a traditional three tier application. This application includes a presentation layer (an ASP.NET web application), a business logic application server, and a SQL Server database. The lower half of the system architecture is a process orchestration and systems integration layer called the Data Import Server.

Figure 8: Unified CCMP Architecture



Web Application

The user interface to Unified CCMP is via a web application that you access using a web browser. You gain access to the Unified CCMP application through a secure sign-in screen. Every user has a unique username. This user is assigned privileges by the system administrator, which defines the system functions the user can access and perform.

The user interface is time-zone aware and connections to it are secured through HTTPS. The web application is hosted on the server by Microsoft Internet Information Services (IIS) so it is suitable for lockdown in secure environments.

Application Server

The Unified CCMP Application Server component provides a secure layer in which all business logic is implemented. The application server component runs in a separate service and is always hosted with the web server component. The application server component also includes caching to improve performance and audits all actions taken by signed-in users.

Reporting Services

Unified CCMP uses Microsoft Reporting Services technology for generating reports. Microsoft Reporting Services is a part of SQL Server Enterprise Edition. Unified CCMP provides a flexible reporting system in which reports are authored in the industry standard Report Definition Language (RDL).

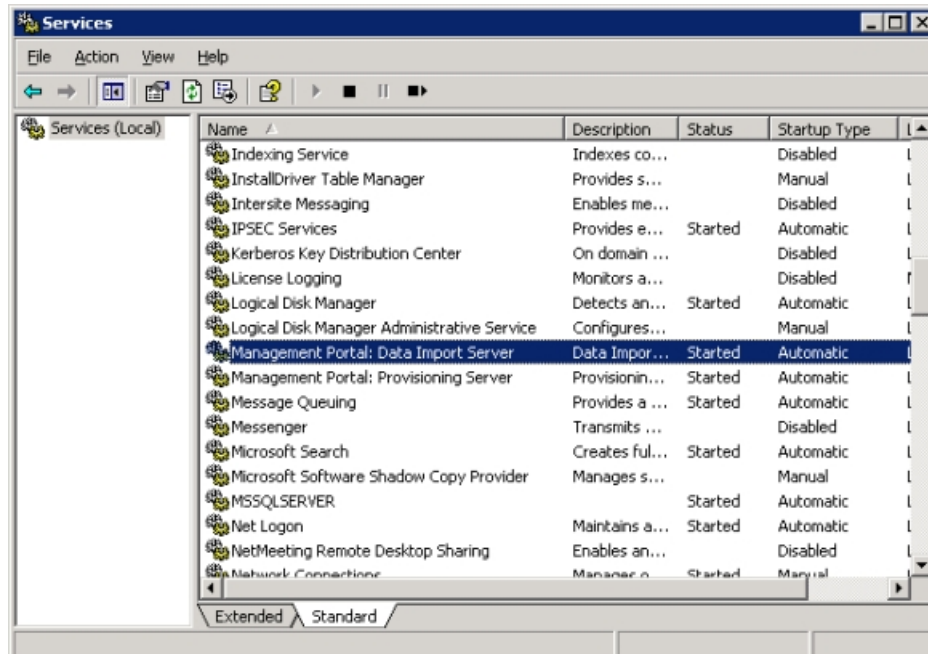
Data Import Server

The Data Import Server component is an Extract, Transform, and Load application for Unified CCMP. The Data Import Server component imports the data used in Unified CCMP. The Data Import Server component is designed to handle high volume data (facts), such as call detail records and data which is changed irregularly (resources), such as agents, peripherals, and skill groups. The Data Import Server component is also responsible for monitoring changes in Unified CCMP system and ensuring that those changes are updated onto Unified ICM/Unified CCE and Unified Communications Manager. The Data Import Server component orchestrates the creation, deletion, and update of resources to Unified ICM/Unified CCE and Unified Communications Manager. The Microflow Runtime is the heart of the Data Import Server component. It orchestrates systems without resorting to low level programming languages. The Microflow Runtime is a general purpose scripting environment and can be applied to a wide range of problems. The term microflow describes any modular, reusable, and independent unit of business logic. An example microflow might update an agent on Unified ICM/Unified CCE when changes are made in the Unified Communications Manager web server component.

Unified CCMP Services

- **Management Portal, Data Import Server:** The Data Import Server is responsible for importing new dimensions and changes to dimensions such as agents, skill groups, call types, and dialed numbers from Unified CCE. The Data Import Server periodically checks whether there are any new dimensions to import or whether there have been any changes made to dimensions that have already been imported. This periodic check allows for closed-loop management of changes made to dimensions provisioned by Unified CCMP.
- **Management Portal, Provisioning Server:** The Provisioning Server is responsible for sending provisioning requests from Unified CCMP to Unified CCE. The requests are move, add, change, and delete (MACD) operations for the resource types that Unified CCMP can manage such as creation of new resources, for example a new agent, or new memberships, such as an Agent to Skill Group membership. These updates are applied via the ConAPI interface.

Figure 9: Unified CCMP Services



Unified CCMP exposes a rich set of performance (known as PerfMon) counters that you can monitor in real time to gauge status, performance and health.

A shortcut to the 32-bit version of Performance Monitor application is available in the Cisco Unified CCE Tools folder for easy access. This shortcut launches the 32-bit version of PerfMon utility so that you can easily monitor the Unified CCE processes.

Outbound Option

Unified ICM and Unified CCE support outbound campaign dialing through its Outbound Dialing subsystem (also known as Blended Agent or BA). The Outbound Dialing subsystem consists of three major components: the Campaign Manager, the Import Process, and the Dialers.

Outbound campaigns start with the Import process. Use the Import process to import a set of outbound calls into the BA database. This data defines what calls are made and how they are made.

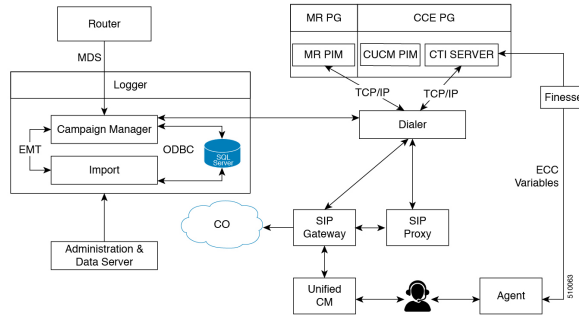
The Campaign Manager is responsible for running the Outbound Dialing campaigns. It reads the campaigns from the BA DB. It then distributes the calls to be made to the Dialers. It takes the results of calls and sends reporting information to the Unified ICM/Unified CCE central controller where it is recorded in Unified ICM/Unified CCE reporting database.

The Outbound Option Dialer maximizes the resources in a contact center by dialing several customers per agent. This component resides on the PG server.

The outbound Option deployment uses the Session Initiation Protocol (SIP) Dialer. The SIP dialer performs dialing, call control, Voice Gateway Interaction functionality instead of using resources on managing the call. In an Outbound Option deployment that uses the SIP Dialer handles the Call Progress Analysis for Outbound campaigns. This helps in increasing the number of outbound agents that a deployment can service on a PG. This reduces the number of PGs and Dialers deployed for larger enterprise systems.

The following diagram provides a high-level view of the Outbound Option components and their relationship with other Unified ICM components.

Figure 10: Outbound Option Component Relationships



Enable the Outbound Option high availability option to provides continuous service without any disruptions, using redundant SIP Dialers and Campaign Managers.



CHAPTER 2

Monitoring SNMP Health

- [SNMP Overview](#), on page 17
- [Base-Level SNMP MIB Support](#), on page 19
- [CISCO-CONTACT-CENTER-APPS-MIB](#), on page 21
- [Configuring the SNMP Agents](#), on page 42

SNMP Overview

Faults

Unified CCE has an internal, proprietary, event management system (EMS) that provides guaranteed delivery of application faults and status events from distributed nodes to the Logger component. Alarms are delivered (via MDS) to the Logger where they are stored in the database; alarms are subsequently forwarded to configured interfaces for external delivery, for instance, to an SNMP network management station (NMS) via SNMP or syslog or both.

SNMP notifications generated by the contact center application are always generated as SNMP traps from the Logger; only generic traps or traps from other subagents (such as the platform subagents provided by Hewlett Packard or IBM) are generated from Unified CCE nodes other than the Logger.

Events destined to be sent beyond just the local trace logs are stored in the local Windows Event log and then forwarded via MDS to the Logger. The Logger stores all received events in the database and then forwards them to the syslog interface (if configured). A subset of the alarms becomes SNMP notifications – only those deemed to be health-impacting are sent to SNMP notification destinations. Thus, all SNMP notifications are sent to syslog collectors; all syslog events are also stored in the Unified CCE database; every event that becomes a syslog event is stored in the Windows Event log on the server that generated the event and it is also stored in the trace log of the process that generated the event.

The following is the format of Unified CCE SNMP notifications (as defined in CISCO-CONTACT-CENTER-APPS-MIB):

```
cccaIcmEvent NOTIFICATION-TYPE
  OBJECTS {
    cccaEventComponentId,
    cccaEventState,
    cccaEventMessageId,
    cccaEventOriginatingNode,
    cccaEventOriginatingNodeType,
    cccaEventOriginatingProcessName,
    cccaEventOriginatingSide,
```

```

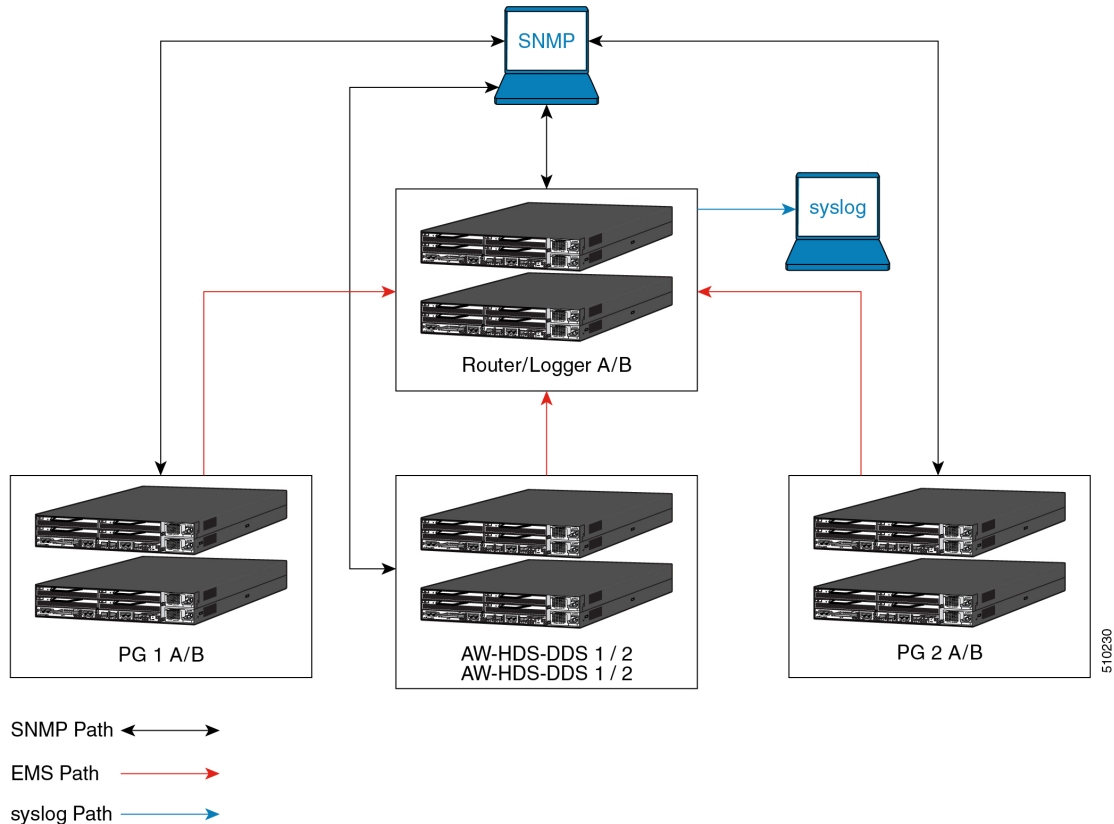
    cccaEventDmpId,
    cccaEventSeverity,
    cccaEventTimestamp,
    cccaEventText
}

```

A detailed description of each object in the notification type is found in [cccaIcmEvent](#), on page 53 .

The following illustration shows the path alarms take from distributed nodes, via the Logger component to an external NMS or alarm collector.

Figure 11: ICM/CCE Event Message Flow



The red lines denote the path that alarms and event messages take within the Unified CCE event management system (EMS). These are one way from component node to the Logger (via the Router). Events are stored in the database and forwarded to the SNMP and syslog interfaces for distribution to configured collectors. Syslog is not supported on any Unified CCE nodes other than the Loggers.

The black lines denote the path of generic, or non-Unified CCE agent, SNMP notifications from device to a configured SNMP management station or stations. These are bidirectional in that SNMP management stations may poll (appropriately configured) devices for instrumentation. (Agents, by default, listen for polls on port 161.) With Unified CCE, SNMP agent processes run at a reduced priority, receiving only idle CPU time slices. As such, agent performance is throttled to ensure that a polling device cannot adversely impact the real-time Unified CCE application processes and cause a failure or impairment.

The blue lines denote the path of syslog events. Only the Loggers may generate syslog events. Syslog events are sent only to configured collectors. If no syslog collector is configured, the CW2KFeed process does not

run and no syslog events are generated. The syslog feed can be quite verbose with more than 1,000 unique events possible depending on deployment model and optional components installed.

There are over 400 configured SNMP notifications for Unified ICM/Unified CCE.

Instrumentation

All Unified CCE servers expose instrumentation defined by the following MIBs:

- MIB-II
- CISCO-CONTACT-CENTER-APPS-MIB
- HOST-RESOURCES-MIB
- SYSAPPL-MIB

The servers may (optionally) expose platform MIBs appropriate for the vendor-originated server model; these MIBs and subagents are provided by the server vendor. If the provided subagent is a Microsoft Windows extension agent (designed to integrate with the Windows SNMP service), it seamlessly integrates with the SNMP agent implementation installed by Unified ICM/Unified CCE.

Tables within the CISCO-CONTACT-CENTER-APPS-MIB are populated depending on which Unified CCE components are installed and configured on the server. If a certain component is not installed, that component-specific table is empty.

Base-Level SNMP MIB Support

SNMP Primary Agent

Unified CCE uses the SNMP Research International EMANATE SNMP agent infrastructure. The agent infrastructure employs typical primary/subagent architecture; the primary agent supports industry-standard MIB-II instrumentation. Subagents service polls for instrumentation from the MIBs listed here. There is also a built-in subagent adapter process that integrates Microsoft Windows extension agents, which operate using the built-in Windows primary/subagent interface. Thus, existing extension agents are seamlessly integrated into the infrastructure.

The SNMP primary agent supports SNMP v1, v2c, and v3. For SNMP v3, the primary agent supports both authentication and privacy, offering MD5 and SHA-1 for authentication and 3DES, AES-192, and AES-256 for privacy.

The primary agent listens for polls on port 161 (gets or sets) and by default, sends traps to the network management station on port 162. You can configure either port other than the well-known ports via the Unified CCE Microsoft Management Console (MMC) snap-in configuration tool.

Base Level SNMP Subagents

The SNMP subagents are processes that provide access to the application instrumentation within the server. The subagents do not interact with the management station directly. Each subagent responds to the get and set requests forwarded to them by the SNMP primary agent.

Platform MIB Support

A platform MIB/subagent is provided by the hardware vendor. This subagent provides instrumentation for low-level attributes of the specific hardware.

Host Resources MIB Subagent

The Host Resources MIB is an implementation of RFC-2790. The Host Resources MIB is a standard MIB which provides attributes common to all hosts, including but not limited to Windows- and Linux-based servers. Thus, the attributes defined are independent of the operating system, network services, or software applications. The instrumentation is focused on host memory, processors, storage devices, run-time system data, and software running on the host.

The Unified CCE Host Resources MIB subagent supports the following MIB objects/tables:

- hrSystem group
- hrMemorySize object
- hrStorage table
- hrDevice table
- hrProcessor table
- hrNetwork table
- hrDiskStorage table
- hrFS table
- hrSWRun table
- hrSWRunPerf table
- hrSWInstalledLastChange object
- hrSWInstalledLastUpdateTime object
- hrSWInstalled table

The Host Resources MIB SNMP Agent is a complete implementation of the Host Resources MIB, proposed standard RFC-1514. The Host Resources MIB is also compliant with Host Resources MIB, draft standard RFC-2790. The agent provides SNMP access to useful host information, such as the storage resources, process table, device information, and the installed software base.

Each `cccaComponentElmtEntry` in the `cccaComponentElmtTable` in the Cisco Contact Center Applications MIB corresponds to a Unified ICM/Unified CCE managed process. The `cccaComponentElmtName` field contains the process executable name without the `.exe` extension. The `cccaComponentElmtRunID` field contains the process ID, which you can use as an index to the Host Resources MIB to obtain current values from the `hrSWRunTable` and `hrSWRunPerfTable` tables. The following example shows the relationship `forcccaComponentElmtRunID.0.1.5 = 5384` using the results in Appendix A and a subset of the results provided by the Host Resources MIB SNMP agent on the same system:

```
cccaComponentElmtName.0.1.5 = router
cccaComponentElmtRunID.0.1.5 = 4040
cccaComponentElmtStatus.0.1.5 = active(5)
hrSWRunIndex.4040 = 4040
hrSWRunName.4040 = router.exe
hrSWRunPath.4040 = C:/icm/bin/router.exe
hrSWRunType.4040 = application(4)
hrSWRunStatus.4040 = notRunnable (3)
hrSWRunPerfCPU.4040 = 20
hrSWRunPerfMem.4040 = 6428
```



Note The implementation approach for standardized MIBs, such as the Host Resources MIB, can vary from vendor to vendor, subject to interpretation. For example, the hrSWRunStatusobject value (notRunnable) shown in the preceding example is subjective; notRunnable implies that the process is not allocated CPU cycles at the precise moment that the MIB was polled. However, any row in the hrSWRunTable indicates a process was loaded and assigned a process ID regardless of whether it is receiving CPU cycles at the moment this object value is polled. Later changes to the SNMP subagent are aligned with this assumption: any process loaded is considered running even it is not allocated CPU cycles.

MIB2

The MIB2 is defined in RFC-1213. It contains objects such as interfaces, IP, ICMP.

This MIB is fully supported on Unified CCE deployments.

SYSAPPL MIB Subagent

The System-Level Managed Objects for Applications MIB (also known as SYSAPPL MIB) is an implementation of RFC-2287. The information allows for the description of applications as collections of executables and files installed and running on a host computer. The MIB enumerates applications installed and provides application run status, associated processes and locations of executables and files on the disk.

The Unified CCE SYSAPPL-MIB subagent supports the following SYSAPPL-MIB objects/tables:

- sysApplInstallPkg table
- sysApplInstallElmt table
- sysApplElmtRun table
- sysApplPastRunMaxRows scalar
- sysApplPastRunTableRemItems scalar
- sysApplPastRunTblTimeLimit scalar
- sysApplElemPastRunMaxRows scalar
- sysApplElemPastRunTableRemItems scalar
- sysApplElemPastRunTblTimeLimit scalar
- sysApplAgentPollInterval scalar
- sysApplMap table – sysApplMapInstallPkgIndex

The SYSAPPL-MIB is a good way to capture a software inventory – applications installed on the server.

The SYSAPPL MIB supports configuration, fault detection, performance monitoring, and control of application software. It contains tables that define an application as a series of processes and services. This includes objects for applications installed on the system, elements and processes that comprise an application, and currently running and previously run applications.

CISCO-CONTACT-CENTER-APPS-MIB

The Cisco Contact Center Applications MIB contains tables of objects for the following Unified ICM/Unified CC components:

- Router (and NICs for Unified ICM)
- Logger

- Peripheral Gateways (PGs) (and PIMs)
- Administration Server and Real-time Data Server (AWs and HDSs)
- CTI Gateways (CGs)
- CTI Object Servers (CTI OS)
- Outbound Option Campaign Manager
- Outbound Option Dialers

The Cisco Contact Center Applications MIB SNMP subagent provides access to component inventory, component status, performance metrics, and links to IETF standard host-based MIBs. Appendix A, section 0 provides an example of the data provided by a Unified ICM/Unified CC installation.

CISCO-CONTACT-CENTER-APPS-MIB Overview

The CISCO-CONTACT-CENTER-APPS-MIB is implemented on all major components of the Unified CCE solution. That is, the Router, Logger, Peripheral Gateway and the AW/HDS.



Note In prior versions, the CTI Gateway and the CTI Object Server components were supported installed on separate servers; however, are now only supported co-located on the Peripheral Gateway.

The SNMP agent infrastructure is installed on all of these component servers with a subagent that serves CISCO-CONTACT-CENTER-APPS-MIB instrumentation for that server. The MIB defines a number of tables of instrumentation – one set for discovery and basic health monitoring and an additional set of tables of component-specific instrumentation. Each common component of a Unified CCE deployment has a table of objects – the Router (with a sub-table of NICs), the Logger, the Administration Server and Real-time Data Server (AW), the PG (with a sub-table of PIMs), and the CG and CTI OS as well as Outbound Option components, Campaign Managers on the Logger and the Dialer on the PG. The component-specific tables are only populated if that component is installed on the server.

CISCO-CONTACT-CENTER-APPS-MIB Structure

At the base, tables in the CISCO-CONTACT-CENTER-APPS-MIB are indexed by the Unified CCE instance (the instance name is a unique textual identifier that relates components that are part of the same Unified CCE system); most are secondarily indexed by the Component index. In a hosted deployment, there may be up to 25 instances of a particular component installed on a single server (such as a router – one for each customer instance in a service provider solution). This is why the Unified CCE instance is the primary index – it is the only way to distinguish one router from another. However, in a typical Unified CCE deployment, there is only a single instance.

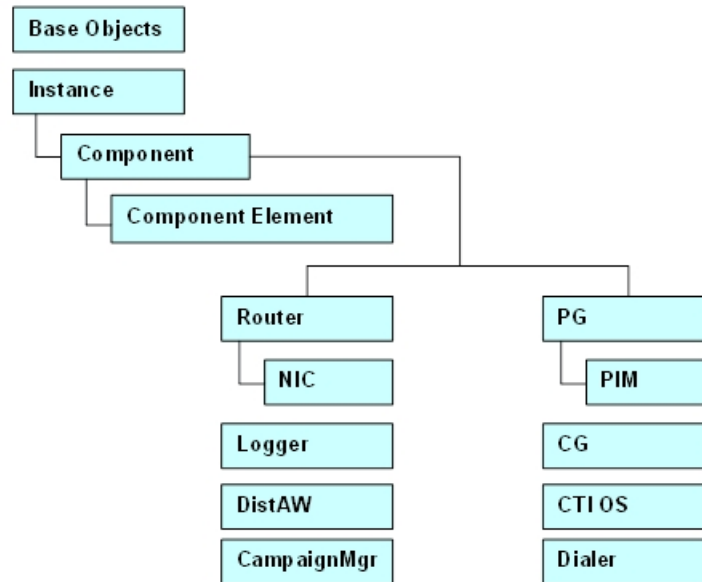
Thus, to inventory a particular server, the NMS should query the Instance table first; then query the Component table to assign components to an instance. Lastly, query the Component Elmt table for the processes associated with each component.

Using the Instance and Component indexes, the NMS can then drill down further using it to query the component-specific instrumentation for each component installed.

The component-specific table of instrumentation provides (where possible) links to dependent components that are distributed within the solution (for example, which Router a peripheral gateway communicates with or which Logger is the primary for a particular Administration Server and Real-time Data Server).

The CISCO-CONTACT-CENTER-APPS-MIB is structured as follows:

Figure 12: CISCO-CONTACT-CENTER-APPS-MIB Structure



The Instance table is indexed by the instance number – a value ranging from 1 to 25.

The Component table is indexed by Instance, and Component number that is arbitrarily assigned by the agent; the value of the Component number could change from one run period to another.

The Component Element table is indexed by Instance, Component number, and Component Element number, which is arbitrarily assigned by the agent; the value of the Component Element number could change from one run period to another.

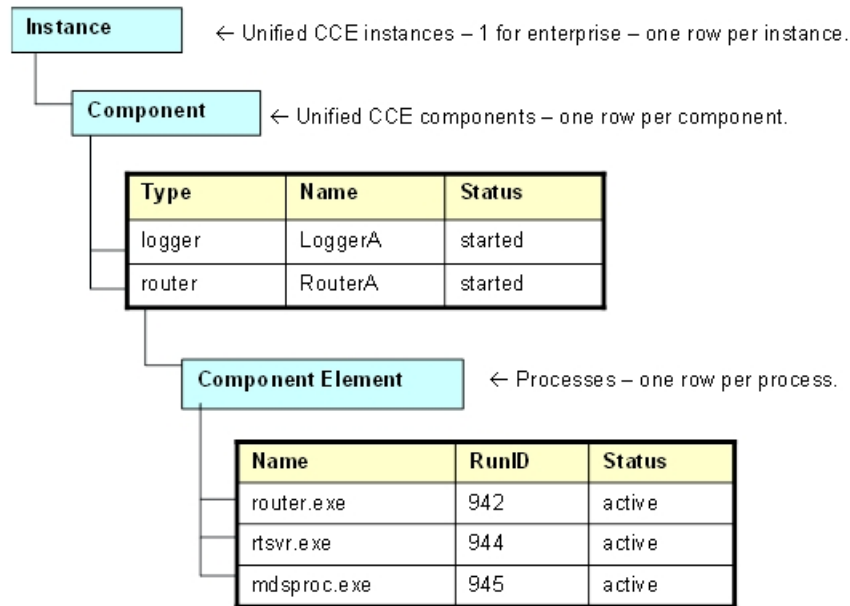
Each component-specific table of instrumentation is indexed by Component number.

From an inventory standpoint (a network management station taking inventory of the server itself), the Network Management Station (NMS) first polls the Instance table. Typically, for Unified CCE, there is only one instance. From that, the NMS polls all components that are part of this instance. Now the NMS knows what is installed on this server and can see what is running. For example, this is a Unified CCE central controller and the NMS wants to know what the inbound call rate is. With the Component entry for the Router, using the Component index of that entry, the NMS then polls the cccaRouterCallsPerSec object within the Router table (indexed by Instance number and Component index).

Additional inventory can be accomplished by drilling a little deeper. For example, assume the NMS wants to list what PIMs are installed on PG4A. Again, poll the Instance table to get the instance number. Using that, get all components for that instance. Find PG4A and using the component index for PG4A, get the PG table objects for PG4A. Then get the PIM table for PG4A that returns a list of PIMs installed.

The following figure illustrates content for the application components installed:

Figure 13: CCA MIB – Component Inventory Example



Typically, for a Unified CCE deployment, a single instance is configured. In this case, all installed/configured components are a part of that same instance.

The Component table comprises a list of installed Unified CCE components (for example, Router and Logger).

The Component Element table is a list of installed processes that should be running.

Real-time status of each component may be monitored by polling the `ccaComponentTable`. The status of a Unified CCE component is derived by analyzing the collective status of each component element (the processes) as best it can.

The Component Element table lists all Unified CCE processes that should be running, and exposes the (operating system) process identifier and the current status of the process.

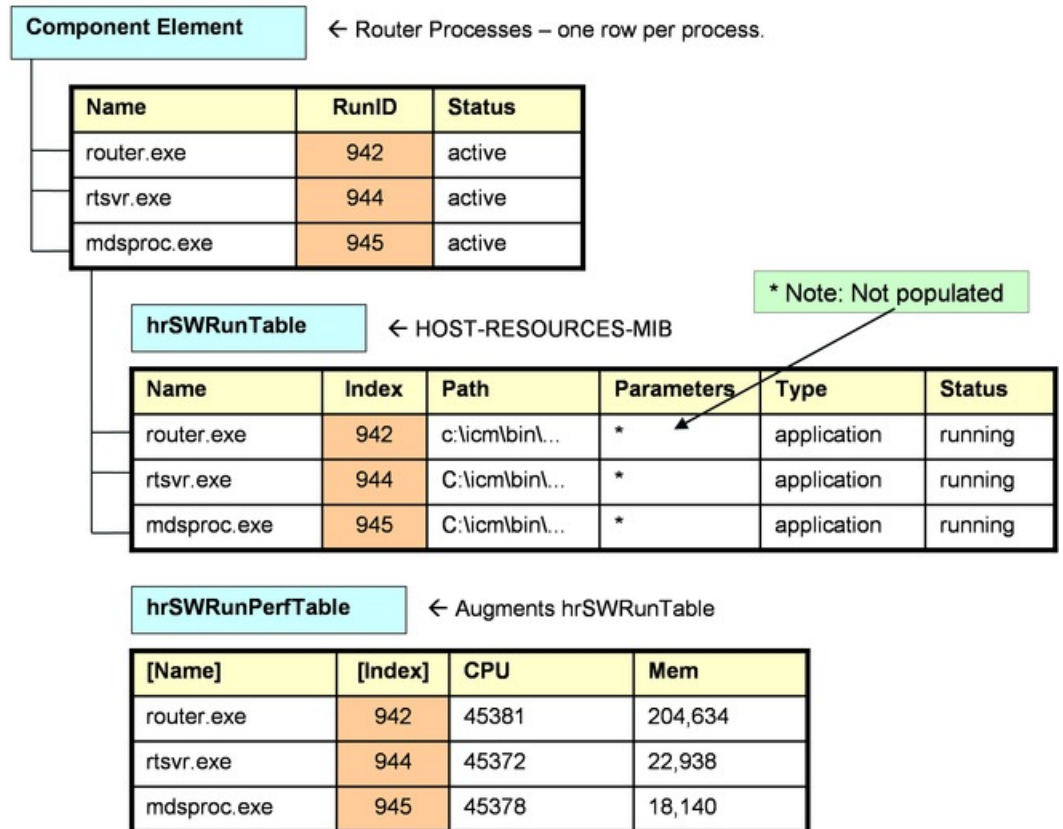


Note The information in the figure is an example, only; there can be many more processes listed in the Component Element table.

Mapping CCA-MIB to Standard Host MIBs

The Component Element table also provides a row-by-row mapping of Unified CCE processes to corresponding rows of instrumentation in the HOST-RESOURCES-MIB and SYSAPPL-MIB. The direct mapping is accomplished using the RunID object. Thus, rather than duplicate instrumentation already provided by the HOST-RESOURCES-MIB and SYSAPPL-MIB, these standard MIBs augment the application MIB with important process-related information.

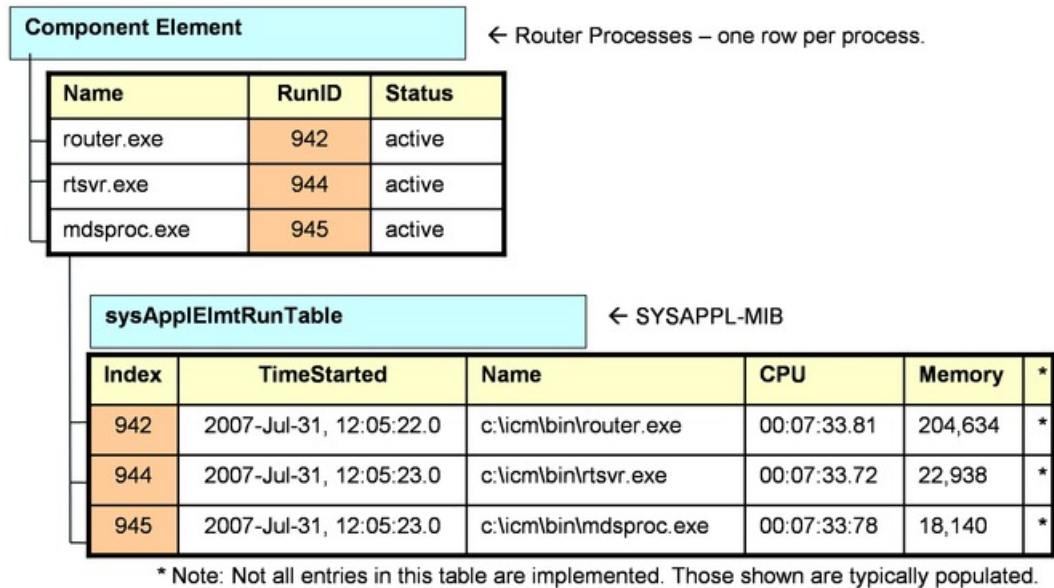
Figure 14: Mapping CCCA MIB Objects to Host MIB Objects



Using the `cccaComponentElmtRunID` object, a monitoring application can use this value as an index into the HOST-RESOURCES-MIB `hrSWRunTable` as well as the `hrSWRunPerfTable` (which augments it). From this, the monitoring application can acquire CPU and memory usage metrics for each process of Unified CCE. The application could also poll the remaining rows of the `hrSWRunTable/hrSWRunPerfTable` for processes that are consuming excessive CPU cycles and/or system memory.

You must note that there is some level of interpretation open to an implementer of a HOST-RESOURCES-MIB subagent. The implementer may decide that some columns of the table cannot be implemented or simply are not necessary. There are no strict rules. That some objects within these tables do not have values is not necessarily indicative of a failed implementation.

Figure 15: Mapping CCCA MIB to SYSAPPL MIB



If a monitoring application prefers to acquire CPU and/or memory metrics on a per-process basis, the `cccaComponentElmtRunID` value may also be used as an index into the SYSAPPL-MIB `sysAppElmtRunTable`.

The component-specific and subcomponent-specific tables include a separate table of instrumentation for each possible Unified CCE component. The list of tables includes:

- Router Table (`cccaRouterTable`)
 - NIC Table (`cccaNicTable`) – because nearly always installed on the Router, this is considered a subcomponent of the Router
- Logger Table (`cccaLoggerTable`)
- Distributor Admin Workstation Table (`cccaDistAwTable`)
- Peripheral Gateway Table (`cccaPgTable`)
 - Peripheral Interface Manager Table (`cccaPimTable`) – because always installed on the PG, this is a subcomponent of the PG
- CTI Gateway Table (`cccaCgTable`)
- CTI Object Server Table (`cccaCtiOsTable`)
- Outbound Option Campaign Manager (`cccaCampaignMgrTable`)
- Outbound Option Dialer (`cccaDialerTable`)

A single notification object is defined in the MIB, which is used to describe the format and content of all notifications generated by Unified ICM and Unified Contact Center.

CISCO-CONTACT-CENTER-APPS-MIB Objects

The following section provides a more detailed description of each object in the CISCO-CONTACT-CENTER-APPS-MIB (CCCA MIB).

CCCA MIB Base Objects

cccaName

The fully-qualified domain name of the enterprise contact center application server.

cccaDescription

A textual description of the enterprise contact center application installed on this server. This is typically the full name of the application.

cccaVersion

Identifies the version number of the enterprise contact center application software installed on this server.

cccaTimeZoneName

The name of the time zone where the enterprise contact center application server is physically located.

cccaTimeZoneOffsetHours

The number of hours that the local time, in the time zone where the enterprise contact center application server is physically located, differs from Greenwich Mean Time (GMT).

cccaTimeZoneOffsetMinutes

The number of minutes that the local time, in the time zone where the enterprise contact center application server is physically located, differs from Greenwich Mean Time (GMT). This object is combined with the `cccaTimeZoneOffsetHours` object to represent the local time zone total offset from GMT.

cccaSupportToolsURL (Deprecated)

The URL for the enterprise contact center application Support Tools application server. The Support Tools application server is an optional component of the solution and offers a centralized server for diagnostic and troubleshooting tools. This application server resides on a Administration Server and Real-time Data Server host. This object offers a navigation point from the management station (assuming a web interface) can quickly access the Support Tools application server.

cccaWebSetupURL

The web setup URL object holds the URL for the enterprise contact center application setup web service. The setup web service is a component of every Unified ICM and Unified CCE server and allows for an administrator to configure parameters of the contact center application as it relates to the installation of the product itself (not to be confused with provisioning).

cccaNotificationsEnabled

The notifications enabled object allows a management station to (temporarily) disable, during run time, all outgoing contact center application notifications. This is typically done during a maintenance window where many application components are frequently stopped, reconfigured and restarted, which can generate periodic floods of notifications that are not desirable during that maintenance period. Note that this setting is persistent even after a restart of the agent; the management station must explicitly reset this object value to true to re-enable outgoing application notifications.

CCCA MIB Instance Table Objects

The instance table is a list of enterprise contact center application instances. Each instance represents a contact center application solution. A solution includes a collection of interconnected functional components (for example, a Router, a Logger and a PG), each of which perform a specific, necessary function of the contact center application.

cccaInstanceNumber

A numeric value that uniquely identifies an enterprise contact center application instance. The instance number is a user-defined value configured when the instance is created by the administrator.

cccaInstanceName

The configured textual identification for the enterprise contact center application instance.

CCCA MIB Component Table Objects

The component table is a list of enterprise contact center application functional components. A Unified CCE solution includes a collection of interconnected functional components (for example, a Router, a Logger and a Peripheral Gateway), each of which perform a specific, necessary function of the contact center application. This table enumerates and lists all contact center application functional components installed and configured on this server.

A single server is permitted to have multiple functional components of a different type, but also multiple components of the same type.

This table has an expansion relationship with the instance table; one or many entries in this table relate to a single entry in the instance table.

cccaComponentIndex

A numeric value that uniquely identifies an entry in the component table. This value is arbitrarily assigned by the SNMP subagent.

cccaComponentType

Identifies the type of enterprise contact center application functional component.

router(1), Logger(2), distAW(3), pg(4), cg(5), ctios(6)

cccaComponentName

A user-intuitive textual name for the enterprise contact center application functional component. Typically, this name is constructed using the component type text, the letter that indicates which side this component represents of a fault tolerant duplex pair and potentially a configured numeric identifier assigned to the component. For example, a Router component might be RouterB; a peripheral gateway might be PG3A. Often, this name is used elsewhere (in contact center application tools) to identify this functional component.

cccaComponentStatus

The last known status of the enterprise contact center application functional component.

Unknown (1)

The status of the functional component cannot be determined.

Disabled (2)

The functional component was explicitly disabled by an administrator.

Stopped (3)

The functional component is stopped. The component may be dysfunctional or impaired.

Started (4)

The functional component was started.

Disconnected (7)

The component is unexpectedly disconnected from a dependent component or service.

Uninitialized (8)

The component has not yet completed its initialization process.

NotRoutable (9)

The component is currently unable to make routing decisions.

CCCA MIB Component Element Table Objects

The component element table provides a list of component (operating system) services or processes that are elements of an enterprise contact center application functional component. Each entry identifies a single process that is a necessary element of the functional component.

This table also provides a one-to-one mapping of entries to a corresponding entry in IETF standard host and application MIB tables. The HOST-RESOURCES and SYSAPPL MIBs expose tables that provide additional instrumentation for software and applications and for the processes that make up that software or those applications. The HOST-RESOURCES-MIB entries in hrSWRunTable and hrSWRunPerfTable and the SYSAPPL-MIB entries in sysAppElmtRunTable have a one-to-one relationship to entries in the component element table. The entries in these standard MIB tables are solely or partially indexed by the operating system process identifier (ID). The process ID is an integer value that uniquely identifies a single process that is currently running on the host. Entries in the component element table maintain its process ID; this value is used to relate the entry to a corresponding entry in the referenced tables of HOST-RESOURCES-MIB and SYSAPPL-MIB.

cccaComponentElmtIndex

A unique numeric identifier for a system process or service that is a necessary element of an enterprise contact center application functional component. This value is arbitrarily assigned by the SNMP subagent.

cccaComponentElmtName

The textual name of the component element, as known by the contact center application. The component element is an operating system process, which is a necessary element of the enterprise contact center application functional component. Most often, this name is the host executable file name, without the file extension.

cccaComponentElmtRunID

The operating system process ID for the process or service that is an element of this enterprise contact center application functional component. The component element run ID maps directly to the hrSWRunIndex value of hrSWRunTable and hrSWRunPerfTable (which augments hrSWRunTable) of the HOST-RESOURCES-MIB and the sysAppElmtRunIndex value of sysAppElmtRunTable of the SYSAPPL-MIB. This object value provides the mechanism for a one-to-one relationship between an entry in the referenced tables of these standard MIBs and an entry in the component element table.

cccaComponentElmtStatus

The last known status of a system process or service that is a necessary element of an enterprise contact center application functional component.

Unknown(1)

The status of the component element cannot be determined.

Disabled(2)

The component element was explicitly disabled by an administrator.

Stopped(3)

The component element is stopped; it may be dysfunctional or impaired.

Started(4)

The component element was started.

Active(5)

The component element is currently running.

Standby (6)

The functional component was started, is currently running and is the hot-standby side of a fault-tolerant duplex pair.

Disconnected (7)

The component is unexpectedly disconnected from a dependent component or service.

Uninitialized (8)

The component has not yet completed its initialization process.

NotRoutable (9)

The component is currently unable to make routing decisions.

CCCA MIB Router Table Objects

The Router table lists each enterprise contact center application Router component configured on this server. Each entry in the table defines a separate Router functional component; a single server is permitted to have multiple Router components for deployments but only has one Router for Unified CCE or Unified ICME deployments.

The Router table has a sparse dependent relationship with the component table. The instance number acts as the primary index for the Router table to properly relate a Router component entry to the appropriate instance entry. The component index acts as the secondary index, relating the entry to the corresponding entry in the component table.

cccaRouterSide

Indicates which of the duplex pair this entry represents of an enterprise contact center application fault tolerant router functional component. The Router side value is either 'A' or 'B'. For simplex configurations, the Router side value defaults to 'A'.

cccaRouterCallsPerSec

Indicates the current inbound call rate; that is, the calculated number of inbound calls per second.

cccaRouterAgentsLoggedOn

The number of contact center agents currently managed by the enterprise contact center application. This does not necessarily represent the number of contact center agents that can receive routed calls, but rather the number of agents for which the application is recording statistical information.

cccaRouterCallsInProgress

Indicates the current number of active (voice) calls being managed by the enterprise contact center application. The calls are in various states of treatment.

cccaRouterDuplexPairName

The hostname of the duplex pair (for example, the other side) server of an enterprise contact center application fault tolerant Router component. If this component is not part of a duplex pair (for example, simplex), the object value is the null string.

cccaRouterNicCount

The number of network interface controllers configured and enabled for this enterprise contact center application Router functional component. There is an imposed architectural limit of 32 configured NICs per Router.

cccaRouterCallsInQueue

The Router calls in queue object indicates the total number of calls queued in all network Voice Response Units (VRUs), from the Router's perspective, including those calls that are in the process of transferring to the VRU for queuing.

cccaRouterAppGwEnabled

The Router application gateway enabled object indicates whether an application gateway is configured and a part of this contact center application deployment. An application gateway provides an external interface to business back-end systems that may be used as external input to call scripting logic, or, that logic which controls how a customer call is handled (routed).

cccaRouterDBWorkerEnabled

The Router database worker enabled object indicates whether a database worker process was configured and is a part of this contact center application deployment. A database worker provides an interface to an external database from which data may be retrieved and used as input to call scripting logic, or, that logic which controls how a customer call is handled (routed).

cccaRouterPGsEnabledCount

The Router PGs enabled count object holds the number of PGs that were enabled for this Router; during usual operation, this is the number of PGs that connect to this Router functional component. There is an imposed architectural limit of 150 peripheral gateways per deployment.

cccaRouterPublicHighAddr

The Router public high address object holds the address of the local high-priority interface of this Router functional component to the public network. The public network interface is exposed outside the realm of the Unified ICM or Unified Contact Center application and is used for the transfer of data between this Router and other functional components of the contact center deployment. This interface is reserved for high-priority messages; network prioritization is typically configured for this interface to ensure a level of quality of service.

cccaRouterPublicNonHighAddr

The Router public non-high address object holds the address of the local interface of this Router functional component to the public network that is used for best effort priority messages. The public network interface is exposed outside the realm of the Unified ICM or Unified CC application and is used for the transfer of data between this Router and other functional components of the deployment. This interface is used for normal-priority messages.

cccaRouterPrivateHighAddr

The Router private high address object holds the address of the local high-priority interface of this Router functional component to the private network. The private network interface is used exclusively by the Unified ICM or Unified Contact Center application for the transfer of synchronization data between duplexed pairs and for the transfer of application data from the Router to the Logger. This interface is reserved for high-priority messages and as much as 90% of the available network bandwidth is allocated to this interface.

cccaRouterPrivateNonHighAddr

The Router private non-high address object holds the address of the local interface of this Router functional component to the private network that is used for best effort priority messages. The private network is used exclusively by the Unified ICM or Unified Contact Center application for the transfer of synchronization data between duplexed pairs and for the transfer of application data from the Router to the Logger. This interface is used for normal-priority messages.

CCCA MIB NIC Table Objects

The NIC table lists the enterprise contact center application network interface controllers enabled on this Router functional component.

The NIC table has an expansion dependent relationship with the Router table. There may be one or more NIC entries associated with a single Router entry. The instance index acts as the primary index and the component index a secondary index. This indexing method ensures that NIC entries are properly related to its parent Router and to the appropriate instance. The SNMP agent arbitrarily assigns the NIC index when each NIC table entry is created.

cccaNicIndex

A value that uniquely identifies an entry in the network interface controller table. The value of this object is arbitrarily assigned by the SNMP subagent.

cccaNicType

Indicates to which telephony network this NIC functional component provides an interface.

cccaNicStatus

The last known status of the enterprise contact center application network interface controller functional component.

CCCA MIB Logger Table Objects

The Logger table lists the enterprise contact center application Logger functional components installed and enabled on this server.

The Logger table has a sparse dependent relationship with the component table. The instance number acts as the primary index for the Logger table to properly relate a Logger component entry to the appropriate instance entry. The component index acts as the secondary index, relating the entry to the corresponding entry in the component table.

cccaLoggerSide

Which of the duplex pair this entry represents, of an enterprise contact center application fault tolerant Logger functional component. The Logger side value is either 'A' or 'B'. For simplex configurations, the Logger side value defaults to 'A'.

cccaLoggerType

Which type of enterprise contact center application Logger, is installed on this server. The Logger type varies based on the configuration of the contact center solution.

cccaLoggerRouterSideAName

The hostname of the side 'A' Router that this enterprise contact center application Logger functional component is associated. The Logger component must be connected to a Router that is part of the same instance.

cccaLoggerRouterSideBName

The hostname of the side 'B' Router that this enterprise contact center application Logger functional component is associated. The Logger component must be connected to a Router that is part of the same instance.

cccaLoggerDuplexPairName

The hostname of the duplex pair (for example, the other side) server of an enterprise contact center application fault tolerant Logger component. If this component is not part of a duplex pair (for example, simplex), the object value is the null string.

The Logger connects to its duplex pair via a private' interface a closed subnet that guarantees a quality of service level that does not impact the performance of the contact center application. This private subnet is not accessible by the management station.

cccaLoggerHDSReplication

Indicates whether the Logger component replicates data to a Administration Server, Real-time and Historical Data Server, and Detail Data Server. If true, the Logger feeds historical data at regular intervals to the HDS for long-term storage. In this configuration, administrator reports are generated by accessing data from the HDS rather than the Logger in order to remove the performance impact of reporting on the Logger.

cccaLoggerAvgDBWriteTime

The Logger average database write time expresses the average amount of time, in 100 nanosecond units, required to write data to a table in the central controller database. This value represents the average time per write of the write operations that occurred in the past second. This object is a good indicator of contention for database access.

CCCA MIB Administration Server and Real-Time Data Server Table Objects

The Administration Server and Real-time Data Server table lists the enterprise contact center application Administration Server and Real-time Data Server functional components installed and enabled on this server.

The Administration Server and Real-time Data Server table has a sparse dependent relationship with the component table. The instance number acts as the primary or the Administration Server and Real-time Data Server table to properly relate an Administration Server and Real-Time Data Server component entry to the appropriate instance entry. The component index acts as the secondary index, relating the entry to the corresponding entry in the component table.

cccaDistAwSide

Which of the duplex pair this entry represents, of an enterprise contact center application fault tolerant distributor administrator workstation functional component. The Administration Server and Real-time Data Server side value is either A or B. For simplex configurations, the Administration Server and Real-time Data Server side value defaults to A.

cccaDistAwType

Which type of enterprise contact center application distributor administrator workstation, is installed on this server. The Administration Server and Real-time Data Server type varies based on the configuration of the contact center solution.

cccaDistAwAdminSiteName

A user-defined textual name that uniquely identifies the location or the configuration of the Administration Server and Real-time Data Server component.

cccaDistAwRouterSideAName

The hostname of the side A Router that this enterprise contact center application Administration Server and Real-time Data Server functional component is associated. The the Administration Server and Real-time Data Server component must be connected to a Router that is part of the same instance. If the side B Router is the active Router and a failure occurs, the side A Router then immediately assumes the role. In this case, the Administration Server and Real-Time Data Server lose their connection to the side B Router and thus use this object value to connect to the side A Router.

cccaDistAwRouterSideBName

The hostname of the side B Router that this enterprise contact center application Administration Server and Real-time Data Server functional component is associated. The Administration Server and Real-time Data Server component must be connected to a Router that is part of the same instance. If the side A Router is the active Router and a failure occurs, the side B Router then immediately assumes the role. In this case, the Administration Server and Real-Time Data Server lose their connection to the side A Router and thus use this object value to connect to the side B Router.

cccaDistAwLoggerSideAName

The hostname of the side A Logger that this enterprise contact center application Administration Server and Real-time Data Server functional component is associated. The Administration Server and Real-time Data Server component must be connected to a Logger that is part of the same instance. If the side B Logger is the active Logger and a failure occurs, the side A Logger then immediately assumes the role. In this case, the Administration Server and Real-time Data Server lose their connection to the side B Logger and thus use this object value to connect to the side A Logger.

cccaDistAwLoggerSideBName

The hostname of the side B Logger that this enterprise contact center application Administration Server and Real-time Data Server functional component is associated. The Administration Server and Real-time Data Server component must be connected to a Logger that is part of the same instance. If the side A Logger is the active Logger and a failure occurs, the side B Logger then immediately assumes the role. In this case, the distributor AW loses its connection to the side A Logger and use this object value to connect to the side B Logger.

cccaDistAwDuplexPairName

The hostname of the duplex pair (for example, the other side) server of an enterprise contact center application fault tolerant Administration Server and Real-time Data Server component. If this component is not part of a duplex pair (for example, simplex), the object value is the null string.

cccaDistAwHDSEnabled

Indicates whether this enterprise contact center application distributor administrator workstation has a historical database server (HDS) configured and enabled. If so, this Administration Server and Real-time Data Server receive replicated data from the Logger at periodic intervals and add the data to the HDS. Client administrator workstations generate reports based on the data in this HDS.

cccaDistAwWebViewEnabled (Deprecated)

Indicates whether this enterprise contact center application distributor administrator workstation has a web-based reporting server (WebView) configured and enabled. Having WebView configured and enabled does not imply that a historical database server is also present on this server; the data may be accessed by the WebView server from a database on a different host.

cccaDistAwWebViewServerName (Deprecated)

The server (universal naming convention [UNC]) name of the server where the enterprise contact center application database resides. This database holds the real-time and/or historical data that is requested when generating reports..

CCCA MIB Peripheral Gateway Table Objects

The PG table lists the enterprise contact center application PG functional components installed and enabled on this server.

The PG table has a sparse dependent relationship with the component table. The instance number acts as the primary index for the PG table to properly relate a PG component entry to the appropriate instance entry. The component index acts as the secondary index, relating the entry to the corresponding entry in the component table.

cccaPgNumber

A user-defined numeric identifier for this enterprise contact center application peripheral gateway.

cccaPgSide

Which of the duplex pair this entry represents of an enterprise contact center application fault tolerant peripheral gateway functional component. The PG side value is either 'A' or 'B'. For simplex configurations, the PG side value defaults to 'A'.

cccaPgRouterSideAName

The hostname of the side A Router that this enterprise contact center application peripheral gateway functional component is associated. The peripheral gateway component must be connected to a Router that is part of the same instance. If the side B Router is the active Router and a failure occurs, the side A Router then immediately assumes the role. In this case, the peripheral gateway loses its connection to the side B Router and thus use this object value to connect to the side A Router.

cccaPgRouterSideBName

The hostname of the side B Router that this enterprise contact center application peripheral gateway functional component is associated. The peripheral gateway component must be connected to a Router that is part of the same instance. If the side A Router is the active Router and a failure occurs, the side B Router then immediately assumes the role. In this case, the peripheral gateway loses its connection to the side A Router and thus use this object value to connect to the side B Router.

cccaPgDuplexPairName

The hostname of the duplex pair (for example, the other side) server of an enterprise contact center application fault tolerant peripheral gateway component. If this component is not part of a duplex pair (for example, simplex), the object value is the null string.

cccaPgPimCount

The number of peripheral interface managers configured and enabled for this enterprise contact center application peripheral gateway functional component.

cccaPgCallsInProgress

The call in progress object shows the number of calls that are currently active and being managed or monitored by this peripheral gateway.

cccaPgAgentsLoggedOn

The agents logged in object shows the number of agents associated with this peripheral gateway that are currently logged in and are being managed or monitored by this peripheral gateway.

cccaPgAgentsReady

The agents ready object shows the number of agents associated with this peripheral gateway that are currently logged in and in a 'Ready' state, for example,, ready to receive calls.

cccaPgAgentsTalking

The agents talking object shows the number of agents associated with this peripheral gateway that are currently logged in and taking a call (in a 'Talking' state).

cccaPgID

The PG identifier is a unique numeric identifier for this enterprise contact center application peripheral gateway. The identifier is assigned by the contact center application.

CCCA MIB Peripheral Interface Manager Table Objects

The PIM table lists the enterprise contact center application PIM configured and enabled on this Peripheral Gateway functional component.

The PIM table depends on both the instance table and the PG table; the instance index acts as the primary index and the PG index a secondary index. This indexing method ensures that PIM entries are properly related to its parent PG and to the appropriate instance.

The PIM table has an expansion dependent relationship with the PG table. There may be one or more PIM entries associated with a single PG entry. The instance index acts as the primary index and the component index a secondary index. This indexing method ensures that PIM entries are properly related to its parent PG and to the appropriate instance. The SNMP agent assigns the PIM number, based upon the configuration, when each PIM table entry is created.

cccaPimNumber

The numeric identifier for this enterprise contact center application PIM. This object value is a user-defined numeric value and is limited to a maximum of 32 because this is the maximum number of PIMs supported on a single peripheral gateway.

cccaPimPeripheralName

The user-defined textual name of the enterprise contact center application PIM. This name uniquely identifies the PIM.

cccaPimPeripheralType

The type of the enterprise contact center application PIM, for example, the brand name and model of the ACD, private branch exchange (PBX), or VRU.

cccaPimStatus

The last known status of the enterprise contact center application peripheral interface manager functional component.

cccaPimPeripheralHostName

The hostname or IP address of the peripheral (the PBX, ACD, or VRU) to which the enterprise contact center application PIM is connected. If there are multiple interfaces to the peripheral, each hostname or IP address is separated by a comma.

CCCA MIB CTI Gateway Table Objects

The CG table lists the enterprise contact center application computer telephony integration (CTI) gateway functional components installed and enabled on this server.

The CTI gateway table has a sparse dependent relationship with the component table. The instance number acts as the primary index for the CTI gateway table in order to properly relate a CTI gateway component entry to the appropriate instance entry. The component index acts as the secondary index, relating the entry to the corresponding entry in the component table.

cccaCgNumber

A numeric identifier for this enterprise contact center application CTI Gateway. This is a user-defined numeric value and may not be identical to the table index.

cccaCgSide

Which of the duplex pair this entry represents of an enterprise contact center application fault tolerant CTI gateway functional component. The CG side value is either 'A' or 'B'. For simplex configurations, the CG side value defaults to 'A'.

cccaCgPgSideAName

The hostname of the side 'A' PG that this enterprise contact center application CTI gateway (CG) functional component is associated. The CG component must be connected to a PG that is part of the same instance. If the side 'B' PG is the active PG and a failure occurs, the side 'A' PG then immediately assumes the role. In this case, the CG loses its connection to the side 'B' PG and thus use this object value to connect to the side 'A' PG.

cccaCgPgSideBName

The hostname of the side 'B' peripheral gateway (PG) that this enterprise contact center application CTI gateway (CG) functional component is associated. The CG component must be connected to a PG that is part of the same instance. If the side 'A' PG is the active PG and a failure occurs, the side 'B' PG then immediately assumes the role. In this case, the CG loses its connection to the side 'A' PG and thus use this object value to connect to the side 'B' PG.

cccaCgDuplexPairName

The hostname of the duplex pair (for example, the other side) server of an enterprise contact center application fault tolerant CTI gateway component. If this component is not part of a duplex pair (for example, simplex), the object value is the null string.

cccaCgOpenSessions

The CG open sessions object indicates the number of sessions (connections) that were established between the CTI Gateway and CTI clients. These are active sessions that are functioning usually.

cccaCgOtherSessions

The CG other sessions objects indicates the total number of sessions (connections) between the CTI Gateway and CTI clients that are not usual, open/active sessions. This includes sessions that are 'opening' (not yet established and initialized), session that are 'closing' (connections being torn down) as well as

sessions that are in an 'unknown' state and sessions that have failed. While this object value fluctuates from time to time, it stabilizes during usual operation. A steadily increasing value indicates a problem that should be investigated.

cccaCgID

The CG number is a unique numeric identifier for this enterprise contact center application CTI gateway. The identifier is assigned by the contact center application.

CCCA MIB CTI OS Table Objects

The CTI OS table lists the enterprise contact center application computer telephony integration object server (CTI OS) functional components installed and enabled on this server.

The CTI OS table has a sparse dependent relationship with the component table. The instance number acts as the primary index for the CTI OS table to properly relate a CTI OS component entry to the appropriate instance entry. The component index acts as the secondary index, relating the entry to the corresponding entry in the component table.

cccaCtiOsServerName

The user-defined textual name assigned to this enterprise contact center application CTI OS component to uniquely identify it.

cccaCtiOsPeripheralName

The unique identifier for the peripheral that the enterprise contact center application CTI OS component is associated. This association links the CTI desktop clients with a particular peripheral PBX.

cccaCtiOsPeripheralType

The peripheral type that the enterprise contact center application CTI OS is associated. This also then identifies the peripheral PBX type that the CTI desktop clients are associated.

cccaCtiOsCgSideAName

The hostname of the side 'A' CTI gateway (CG) that this enterprise contact center application CTI object server (CTI OS) functional component is associated. The CTI OS component must be connected to a CG that is part of the same instance. If the side 'B' CG is the active CG and a failure occurs, the side 'A' CG then immediately assumes the role. In this case, CTI OS loses its connection to the side 'B' CG and thus use this object value to connect to the side 'A' CG.

cccaCtiOsCgSideBName

The hostname of the side 'B' CTI gateway (CG) that this enterprise contact center application CTI OS functional component is associated. The CTI OS component must be connected to a CG that is part of the same instance. If the side 'A' CG is the active CG and a failure occurs, the side 'B' CG then immediately assumes the role. In this case, CTI OS loses its connection to the side 'A' CG and thus use this object value to connect to the side 'B' CG.

cccaCtiOsPeerName

The hostname of the peer server of an enterprise contact center application CTI object server functional component. If this component does not have a peer, the object value is the null string. Note that the CTI OS component implements fault tolerance slightly differently than other components of the contact center solution. CTI OS maintains two active peer object servers to serve client desktop CTI applications. If a failure occurs on one of the two servers, its clients connect to the peer server.

cccaCtiOsActiveClients

The active clients object holds the number of CTI OS active client mode desktop connections. This value indicates the total number of desktops connected to the CTI OS server. The number of desktops connected to the A and B side of CTI OS determine the total desktops connected through this instance of CTI OS server.

cccaCtiOsActiveMonitors

The active monitors object holds the number of CTI OS active monitor mode desktop connections. CTI OS only supports two monitor mode connections per each CTI OS server. This value indicates how many monitor mode connections are in use. After there are two in use further monitor mode connection attempts are rejected.

cccaCtiOsCallsInProgress

The calls in progress object indicate the total number of active calls being tracked by CTI OS. This value shows how many calls are currently being handled by CTI OS. This value should go up and down based on the call arrival rate and the agent call completion rate.

cccaCtiOsCallsFailed

The calls failed object holds the total number of calls that failed via a failure event being reported to CTI OS. If this count begins to rise, the log file should be captured to gather more specific information about the failure events.

CCCA MIB Outbound Option Campaign Manager Table Objects

The Campaign Manager table lists the enterprise contact center application Outbound Option Campaign Manager functional components installed and enabled on this server. In virtually all single-instance enterprise deployments, the Campaign Manager is coresident with the Logger.

The Campaign Manager table has a sparse dependent relationship with the component table. The instance number acts as the primary index for the Campaign Manager table to properly relate a Campaign Manager component entry to the appropriate instance entry.

The component index acts as the secondary index, relating the entry to the corresponding entry in the component table.

The SNMP agent constructs the Campaign Manager table at startup. Because you can only configure Campaign Manager components while the enterprise contact center application is stopped, Campaign Manager table entries cannot be added to or deleted from the table either by the agent or the management station when the application is running. The agent updates the values of Campaign Manager entry objects as their values change when the application is running. All objects in this table are read-only to the management station.

Each Campaign Manager entry represents an enterprise contact center application Campaign Manager server functional component configured on the server. The Campaign Manager component, which resides on the Unified ICM/Unified CCE Logger, is responsible for:

- Managing when a campaign runs
- Maintaining system and Dialer configurations
- Making decisions about which contact records to retrieve from a campaign based on configurable query rules and then delivering those contact records to Dialers
- Distributing configuration data to the import process and all available Dialers in the system
- Collecting real-time and historical data and sending it to the Router for subsequent storage and distribution
- Managing the Do Not Call list, ensuring no numbers on it are sent to the Dialers

The objects in each campaign manager entry provide configuration, performance, and component status information.

cccaCampaignMgrDbUtilization

The campaign manager and Import processes share a private database on the Logger. The campaign manager database utilization object shows what percentage of allocated space in the database is currently utilized. An administrator should monitor this object when its value exceeds 80 percent.

cccaCampaignMgrQueueDepth

The campaign manager is a multithreaded process. One main dispatch thread is involved in most processing. The queue depth object indicates how many messages are queued to this internal dispatch thread.

cccaCampaignMgrAvgQueueTime

The campaign manager is a multithreaded process; however, there is one main dispatch thread that is involved in most message processing. The average queue time object shows the average amount of time a message spends in the main dispatch thread queue awaiting processing (in milliseconds).

cccaCampaignMgrActiveDialers

The campaign manager process feeds several Dialer components which manage the dialing of customers for outbound campaigns. The active Dialers counter indicates how many Dialers are currently registered to this campaign manager.

CCCA MIB Outbound Option Dialer Table Objects

The Dialer table lists each enterprise contact center application Outbound Option Dialer component configured on this server. Each entry in the table defines a separate Dialer functional component.

The Dialer table has a sparse dependent relationship with the component table. The instance number acts as the primary index for the Dialer table to properly relate a Dialer component entry to the appropriate instance entry. The component index acts as the secondary index, relating the entry to the corresponding entry in the component table.

The SNMP agent constructs the Dialer table at startup. Because you can only configure a Dialer while the enterprise contact center application is stopped, Dialer table entries cannot be added to or deleted from the table either by the agent or the management station when the application is running. The agent updates Dialer entry objects as their values change when the application is running. All objects in this table are read-only to the management station.

Each Dialer entry represents an enterprise contact center application Outbound Option Dialer functional component configured on the server. The Dialer component maximizes the resources in a contact center by dialing several customers per agent. The Dialer component resides on the peripheral gateway (PG) server, where it does the following:

- Dials customers
- Reserves agents
- Performs call classification
- Calculates agent availability
- Keeps Outbound Dialing at a level where the abandon rate is below the maximum allowed abandon rate

The objects in the Dialer entry provide information about dependent components, performance metrics, and port usage.

cccaDialerCampaignMgrName

The Dialer campaign manager name object holds the hostname or IP address of the Outbound Option Campaign Manager to which this Dialer is associated. The Dialer connects to the campaign manager to exchange data related to an Outbound Dialing campaign.

cccaDialerCampaignMgrStatus

The Dialer campaign manager status indicates the current connection status between this Dialer and the Outbound Option Campaign Manager component, which is coresident with the Logger.

cccaDialerCtiServerAName

The Dialer CTI server A name object holds the hostname or IP address of the contact center application CTI Server side A functional component, which this Dialer depends. The Dialer connects to the CTI Server to monitor skill group statistics (to choose an agent) and runs call control after an available agent is selected.

cccaDialerCtiServerBName

The Dialer CTI server B name object holds the hostname or IP address of the contact center application CTI Server side B functional component, which this Dialer depends. The Dialer connects to the CTI Server to monitor skill group statistics (to choose an agent) and runs call control after an available agent is selected.

cccaDialerCtiServerStatus

The Dialer CTI server status indicates the current connection status between this Dialer and the active CTI server component.

cccaDialerMediaRouterStatus

The Dialer media Router status indicates the current connection status between this Dialer and the Media Routing (MR) Peripheral Interface Manager (PIM) component. The Dialer uses the MR PIM interface to reserve an available agent as a recipient for a dialed customer call.

cccaDialerQueueDepth

The Dialer is a multithreaded process that communicates between threads using inter-thread messaging. The queue depth object indicates how many messages are currently queued for the main dispatch thread. When this object is used in combination with the average queue time object, message processing performance can be gauged.

cccaDialerAvgQueueTime

The Dialer is a multithreaded process that communicates between threads using messaging. One main dispatch thread is involved in most message processing. The average queue time shows the average amount of time (in milliseconds) that a message spent in the queue before being de-queued processing. When this object used in combination with the queue depth object, message processing performance can be gauged.

cccaDialerTalkingAgents

For an agent campaign, the Dialer places calls to customers and transfers those customer calls to agents. The talking agents object indicates how many agents are currently talking in the monitored campaign skill group.

cccaDialerCallAttemptsPerSec (Deprecated)

The call attempts per second object tracks how many calls the Dialer is placing per second, rounded to the nearest integer. If the dialing rate is too high, it can result in network congestion on the voice network, which can result in inefficient dialing.

cccaDialerConfiguredPorts

The Dialer configured ports object is a count of the total number of ports that are configured for placing calls to customers and for transferring calls to agents during outbound calling campaigns. During usual operation, the Dialer configured ports object value is equal to a sum of busy and idle ports.

cccaDialerBusyCustomerPorts

The Dialer busy customer ports object is a count of the number of ports currently in use for customer calls. The port is the unit on the Dialer that places calls to reserve agents and to contact customers.

cccaDialerBusyReservationPorts

The Dialer busy reservation ports object tracks how many ports are currently busy reserving agents. The port is the unit on the Dialer that places calls to reserve agents and to contact customers.

cccaDialerIdlePorts

The Dialer idle ports object is a count of the number of ports that are currently idle, for example, there are no calls to customers or to agents using these ports and they are available to the Dialer for placing new calls.

cccaDialerBlockedPorts

The Dialer blocked ports object is a count of the number of ports that are currently unusable for placing calls. A blocked port may be an impaired or inoperable port or one that has a 'stuck' call that was not dropped. A 'stuck' call is a call that is identified by the application as exceeding a duration threshold.

Configuring the SNMP Agents

Installation Prerequisites for SNMP Support

Unified ICM/Unified CCE SNMP support is automatically installed during setup. No extra steps must be taken during setup for SNMP support to be enabled. However, you must install Microsoft Windows SNMP optional components on the Unified ICM/Unified CCE servers for any SNMP agents to function.



Note Install the appropriate Microsoft Windows SNMP components before you install any Unified ICM/Unified CCE components that require SNMP monitoring. Instructions for installing the Microsoft Windows SNMP component are below.

You require the Microsoft SNMP components are required for Cisco SNMP support. However, the Microsoft Windows SNMP service is disabled as part of the Unified ICM setup and is replaced by the Cisco Contact Center SNMP Management service to process SNMP requests in its place. The Cisco Contact Center SNMP Management service provides for more sophisticated SNMP capabilities than the standard Microsoft SNMP Service.



Note The AppInfo feature provided by the VMware tools has to be disabled. For instructions to disable the AppInfo feature, see the VMware documentation.

SNMP Agent Configuration

While all SNMP components are installed and enabled by default, the device is not manageable via an NMS until you properly configure the solution. You configure the Cisco Contact Center SNMP solution using a Microsoft Management Console (MMC) snap-in. There are many functions of a Windows-based server that are configured using an MMC snap-in so the interface is familiar.

Add Cisco SNMP Agent Management Snap-In

Before you begin

To configure the Cisco SNMP agents, you must first add the Cisco SNMP Agent Configuration snap-in to a Microsoft Management Console. You can then change and save SNMP agent settings. To add the snap-in:

Procedure

- Step 1** From the Start menu select **Run**.
 - Step 2** In the Start box type in `mmc /32` and press **Enter**.
 - Step 3** From the Console, select **File > Add/Remove Snap-in**
A new window appears.
 - Step 4** From the **Standalone** tab, verify **Console Root** is selected in the **Snap-ins added to:** field and click **Add**.
 - Step 5** In the Add Snap-in window scroll down and select **Cisco SNMP Agent Management**.
 - Step 6** In the Add Snap-in window click **Add**.
 - Step 7** In the Add Snap-in window click **Close**.
 - Step 8** Click **OK** in the Add/Remove Snap-in window.
-

The Cisco SNMP Agent Management snap-in is now loaded in the console.

Save Snap-In View

After you load the Cisco SNMP Agent Management MMC Snap-in, you can save that console view to a file (with an .MSC file extension) that you can launch directly instead of repeatedly adding the Snap-in to a new MMC console view.

Procedure

- Step 1** Click **Console > Save As**.

Save As dialog appears.

Step 2 Enter a memorable file name.

Example:

Cisco SNMP Agent Management.msc

Retain the .msc file extension.

Step 3 Click **OK** to save the file to the desired location.

The Administrative Tools (start) menu is the default location, which makes it conveniently available for later access via the Start menu.

Configure Community Names for SNMP v1 and v2c

If you are using SNMP v1 or v2c you must configure a Community Name so that Network Management Stations (NMSs) can access the data provided by your server. These names are left blank during installation for security reasons.

SNMP Community Names are used to authenticate data exchange of SNMP information. An NMS can exchange SNMP information only with servers that use the same Community Name.

To configure the Community Name for SNMP v1 and v2c:

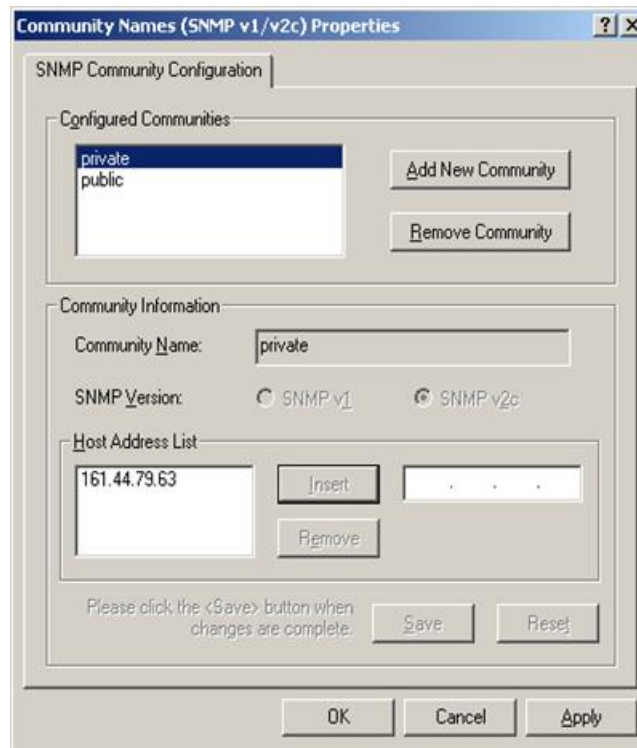
Procedure

Step 1 Expand **Cisco SNMP Agent Management** in the left pane of the MMC snap-in.

Step 2 Highlight **Community Names (SNMP v1/v2c)** in the left pane under Cisco SNMP Agent Management. Community Name, SNMP Version, and Restricted Access columns appear in the right pane.

Step 3 Right-click the white space in the right pane and choose **Properties**.
A dialog box appears.

Figure 16: SNMP Community Name Configuration Dialog



- Step 4** Click **Add New Community**.
- Step 5** In the dialog box, under **Community Information**, provide a community name.
- Step 6** Select the **SNMP Version** by selecting the radio box for SNMP v1 or SNMP V2c.
- Step 7** Optionally, enter one or more IP addresses in the IP Address entry field (containing “dots”) and click **Insert** to enable the access solely for this community from the NMS with the IP Address provided.
- This applies to both polling and traps.
- Step 8** Click **Save**.
- The community name appears in the Configured Communities section at the top of the dialog box.
- Note** You can remove the community name by highlighting the name in the Configured Communities section and clicking Remove Community.
- Step 9** Click **OK**.

Configure User Names for SNMP v3

If you are using SNMP v3 you must configure a User Name so that Network Management Stations (NMSs) can access the data provided by your server. By default, these names are left blank for security reasons.

Procedure

- Step 1** Expand **Cisco SNMP Agent Management** in the left pane of the MMC snap-in.
- Step 2** Highlight **User Names (SNMP v3)** in the left pane under Cisco SNMP Agent Management. User Name, Authentication, Privacy, and Restricted Access columns appear in the right pane.
- Step 3** Right-click the white space in the right pane and choose **Properties**. User Names (SNMP v3) Properties dialog box appears.

Figure 17: SNMP User Name Configuration Dialog Box

- Step 4** Click **Add User**.
- Step 5** Enter user name in **User Configuration** text box .
- Step 6** (Optional) Check **Required?** under Authentication to use SNMP v3 authentication.
- choose an authentication protocol
 - Enter and confirm a password.

Note This setting encrypts the password information as it is sent over the network. You must use these settings on your NMS to access SNMP data from this server.

- Step 7** (Optional) Check **Required?** under Privacy to use SNMP v3 privacy.
- Choose an encryption type.
 - Enter and confirm a password.

Note This setting encrypts all SNMP information as it is sent over the network. If privacy is configured, authentication is required, but you can configure authentication without configuring privacy. You must use these settings on your NMS to access SNMP data from this server.

Step 8 (Optional) Enter one or more IP addresses in the IP Address entry field (containing dots) and click **Insert** to enable access solely from the NMS with the IP Address provided.

This applies to both polling and traps.

Step 9 Click **Save**
The new User Name appears in the **Configured Users** section at the top of the dialog box.

Note You can remove the user by highlighting the name in the Configured Users section and clicking **Remove User**.

Step 10 Click **OK**.

Configure General Information Properties

You can configure general information properties for Cisco SNMP within the Cisco SNMP Agent Management Snap-in.

Procedure

- Step 1** Highlight **General Information** in the left pane under Cisco SNMP Agent Management. Attribute, Value, and Description columns appear in the right pane.
- Step 2** Right-click the white space in the right pane and choose **Properties**. General Information Properties dialog appears.

Figure 18: SNMP General Information Configuration Dialog Box

Step 3 Change the following properties in the **SNMP System Information** section of the General Information Properties dialog box.

Table 1: SNMP General Information Properties

Property	Description
System Name	The fully qualified domain name of the system. If empty, this automatically fills.
System Location	The physical location of the server itself, for example, Building 5, Floor 3, Room 310.
System Contact	The name, email address and/or telephone number of the system administrator or point of contact that should be notified to help resolve a problem with the server.
System Description	A brief description of this server, to include the primary application running on the server.
Number	The port number to be used to access/poll the device. The default port for SNMP polling is UDP 161; if you NMS uses a different port, enter the desired port number here.
Enable Authentication Traps	Check if you wish to enable Authentication Traps. When an NMS attempts to poll this device with inappropriate authentication credentials (for example, wrong community name), the device generates a failed authentication trap.

Note The notifications are explained in
 <INSTALL_DRIVE>/icm/snmp/CCA-Notifications.txt.

- Step 4** (Optional) Change Windows Execution Priority of Cisco SNMP agents in **Agent Performance** section under **Execution Priority**.
The default is Below Normal. You can further lower it by setting it to Low. Keep the settings at the default levels unless you are seeing a significant performance impact.
- Step 5** (Optional) Modify SNMP Agent Performance by changing the number of Concurrent Requests, Subagent Wait Time (in seconds), and Subagents.
The default values are 5, 25, and 25 respectively. Keep the settings at the default levels unless you are seeing a significant performance impact.
-

Maximum Limits Settings for Agent Performance

Specify maximum limits for agent performance in the **General Information Properties** dialog.

Concurrent Requests

The maximum number of SNMP requests that a subagent can currently process. Any pending requests above this value are queued.

Subagent Wait Time

The maximum number of seconds that the primary agent waits for a subagent response.

Subagents

The maximum allowable subagents that the primary agent loads.

Change Agent Log Quantity Setting



Important Change this value only under direction from Cisco Technical Assistance (TAC).

Procedure

- Step 1** Change **Agent Log Quantity** setting in **General Information Properties** dialog.
- **Verbose** (most information),
 - **Normal** (default), or
 - **Terse** (least information)
- Note** You can retrieve logs using the Analysis Manager.
- Step 2** Click **OK** to save changes.
-

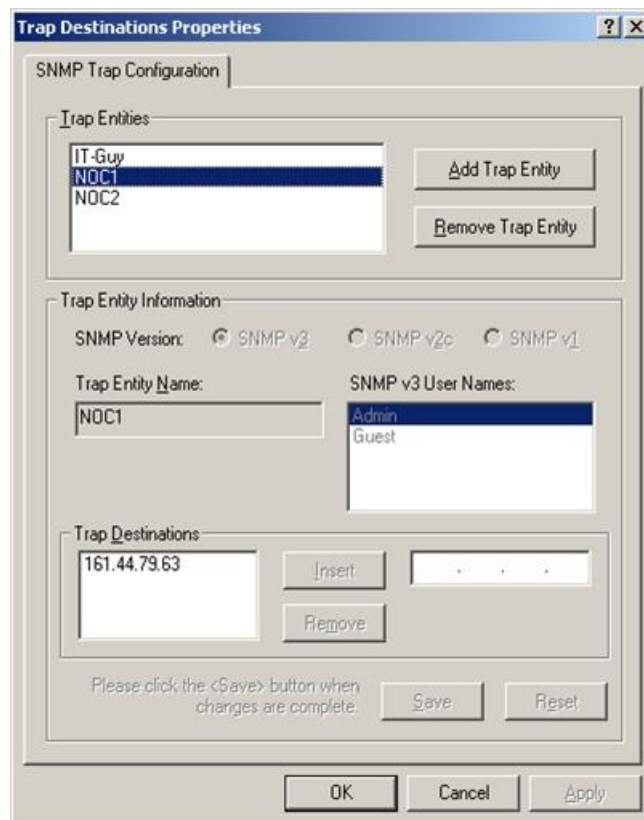
Configure SNMP Trap Destinations

You can configure SNMP Trap Destinations for SNMP v1, SNMP v2c, and SNMP v3. A trap is a notification used by the SNMP agent to inform the NMS of a certain event.

Procedure

- Step 1** Expand **Cisco SNMP Agent Management** in left pane of MMC snap-in.
- Step 2** Highlight **Trap Destinations** in left pane under Cisco SNMP Agent Management. Trap Entity Name and SNMP Version columns appear in the right pane.
- Step 3** Right-click white space in right pane and select **Properties**. A dialog box appears:

Figure 19: SNMP Trap Destination Configuration Dialog Box



- Step 4** Click **Add Trap Entity**.
- Step 5** Select SNMP version in **Trap Entity Information** for version of SNMP used by your NMS.
- Step 6** Provide name for trap entity in **Trap Entity Name** field.
- Step 7** Select user or community name to associate with trap. This list is auto-populated with existing users/community names that have been configured.
- Step 8** Enter IP addresses in IP address entry field (containing “dots”) and click **Insert** to define one or more destinations for traps.
- Step 9** Click **Save** to save trap destination. The Trap Entity Name appears in the **Trap Entities** section at the top of the dialog box.

Note You can remove the Trap Entity by highlighting the name in the **Trap Entities** section and clicking **Remove Trap Entity**.

Step 10 Click **OK**.

Multihomed Windows Server

A multihomed server is a server that connects to multiple network interfaces or IP addresses. If your Microsoft Windows Server uses several IP addresses, you cannot guarantee that the SNMP primary agent binds to the appropriate IP address.

For example, on Unified CCE Routers or Router/Logger (Rogger) systems, **SNMP get** requests may arrive on the public nonhigh priority interface although responses are sent on the public high interface. Also, outbound SNMP traps may be sent using the public high interface when the network management station expects the SNMP traps sent using the public nonhigh priority interface.

There are two ways to bind the SNMP primary agent to the appropriate IP address:

- Continue to use the public high-priority network interface. Configure the network management station to poll the public high interface.
- Use Web Setup to change the IP addresses for the Routers. Use the public high network interface for public (normal priority) traffic. Use the public nonhigh interface for high priority traffic. Ensure that you specify the appropriate priority (high or normal) for all nodes.



CHAPTER 3

Understanding SNMP Notifications

- [Unified ICM/Unified CCE Notification Type](#), on page 53
- [Dual State Objects](#), on page 56
- [Correlating Notifications](#), on page 58
- [Single State Objects](#), on page 59
- [Organizing SNMP Notifications](#), on page 60
- [CSFS Heartbeat Notification](#), on page 60

Unified ICM/Unified CCE Notification Type

cccalcmEvent

An ICM event is a notification that is sent by a functional component of the Cisco Unified Intelligent Contact Management (Unified ICM) and the Cisco Unified Contact Center Enterprise (Unified CCE) contact center applications.

The following table details the objects which comprise the notification type:

Table 2: Unified ICM/Unified CCE Notification Type Objects

Object Name	Description
cccaEventComponentId	A unique identifier used to correlate multiple notifications generated by a single enterprise contact center application functional component or subcomponent. A functional component constructs its unique identifier based upon configured parameters; all notifications by that component include this event component ID.

Object Name	Description
cccaEventState	<p>The state (not to be confused with severity) of the notification and potentially the current state of the functional component that generated the notification. The possible states are:</p> <p>'clear' (0): The clear state indicates that the condition that generated a previous raise notification is resolved.</p> <p>'applicationError' (2): The application error state alerts the recipient that an error exists in the enterprise contact center application but that the error does not affect the operational status of the functional component.</p> <p>'raise' (4): A raise state identifies a notification received because of a health-impacting condition, such as a process failure. A subsequent clear state notification follows when the error condition is resolved.</p> <p>'singleStateRaise' (9): The single state raise state indicates that a health-impacting error occurred and that a subsequent clear state notification is not forthcoming. An example of a single state raise condition is an application configuration error that requires the system to be stopped and the problem resolved by an administrator before the affected component functions properly.</p>
cccaEventMessageId	<p>The unique notification message identifier (value) that was assigned by the enterprise contact center application. This identifier is unique for each different notification but consistent for each instance of the same notification.</p>
cccaEventOriginatingNode	<p>The application-defined name of the enterprise contact center application functional component that generated this notification. This name varies, both in content and in format, based on the component that generated the notification. For example, the name for a Router component may be 'RouterA', a combination of the component identification and the 'side' identifier, while the name 'PG1A' is a combination of the peripheral gateway acronym followed by the peripheral gateway number and the 'side' identifier.</p>

Object Name	Description
cccaEventOriginatingNodeType	<p>The type of enterprise contact center application functional component or subcomponent that generated this notification. The node types are:</p> <p>'unknown' (0): The notification originates from an unknown source.</p> <p>'router' (1): The notification was generated by the Router functional component.</p> <p>'pg' (2): The notification was generated by the peripheral gateway functional component.</p> <p>'nic' (3): The notification was generated by the network interface controller functional component.</p> <p>'aw' (4): The notification was generated by the administrator workstation functional component.</p> <p>'logger' (5): The notification was generated by the Logger functional component.</p> <p>'listener' (6): The notification was generated by the listener functional component. The listener is an enterprise contact center application process that collects event messages from the Logger for display in a Cisco proprietary event management application that is part of the Remote Management Suite (RMS).</p> <p>'cg' (7): The notification was generated by the CTI gateway functional component.</p> <p>'ba' (8): The notification was generated by the Blended Agent functional component. Blended Agent is an enterprise contact center 'outbound option' functional component that manages campaigns of Outbound Dialing.</p>
cccaEventOriginatingProcessName	<p>Each enterprise contact center application functional component includes one or more operating system processes, each of which performs a specific function. The event originating process object identifies the name of the application process that generated this notification.</p>
cccaEventOriginatingSide	<p>The enterprise contact center application functional component fault tolerant side (either 'A' or 'B') that generated this notification.</p>
cccaEventDmpId	<p>The Device Management Protocol (DMP) is a session layer protocol used for network communication between enterprise contact center application functional components. The DMP ID uniquely identifies the session layer addresses of an application functional component. A single component may have multiple DMP IDs because a functional component communicates with other functional components (or its duplex pair) via multiple physical network interfaces and maintain multiple DMP session connections on each interface. Should a communications failure occur, the event DMP ID identifies the physical and logical address that the error occurred.</p>

Object Name	Description
cccaEventSeverity	The severity level of this notification. The severity levels are: 'informational' (1): The notification contains important health or operational state information that is valuable to an administrator; however, the event itself does not indicate a failure or impairment condition. 'warning' (2): The notification contains serious health or operational state information that could be a precursor to system impairment or eventual failure. 'error' (3): The notification contains critical health or operational state information and indicates that the system has experienced an impairment and/or a functional failure.
cccaEventTimestamp	The date and time that the notification was generated on the originating node.
cccaEventText	The full text of the notification. This text includes a description of the event that was generated, component state information, and potentially a brief description of administrative action that may be necessary to correct the condition that caused the event to occur.

Dual State Objects

Most objects are defined as dual state; they have either a raise or clear state. The raise state indicates that there is a problem or fault associated with the object. The clear state indicates the object is operating as usual.

A dual state Unified ICM/Unified CCE SNMP notification contains a raise(4) or clear(0) value in the cccaEventState field. In some cases, multiple raise notifications can correlate to the same object. For example, an object can go offline for a variety of reasons: process termination, network failure, software fault, and so on. The SNMP notification cccaEventComponentId field specifies a unique identifier that you can use to correlate common raise and clear notifications to a single managed object.

The following example shows a pair of raise and clear notifications with the same cccaEventComponentId.



Note The first notification has a raise state; the notification that follows has a clear state.

```
snmpTrapOID.0 = cccaIcmEvent
cccaEventComponentId = 4_1_CC-RGR1A_ICM\acme\RouterA
cccaEventState = raise(4)
cccaEventMessageId = 2701295877
cccaEventOriginatingNode = CC-RGR1A\acme
cccaEventOriginatingNodeType = router(1)
cccaEventOriginatingProcessName = nm
cccaEventOriginatingSide = sideA(1)
cccaEventDmpId = 0
cccaEventSeverity = warning(2)
cccaEventTimestamp = 2006-03-31,14:19:42.0
cccaEventText = The operator/administrator has shutdown the ICM software on
ICM\acme\RouterA
```

```
snmpTrapOID.0 = cccaIcmEvent
cccaEventComponentId = 4_1_CC-RGR1A_ICM\acme\RouterA
```

```

cccaEventState = clear(0)
cccaEventMessageId = 1627554051
cccaEventOriginatingNode = CC-RGR1A\acme
cccaEventOriginatingNodeType = router(1)
cccaEventOriginatingProcessName = nm
cccaEventOriginatingSide = sideA(1)
cccaEventDmpId = 0
cccaEventSeverity = informational(1)
cccaEventTimestamp = 2006-03-31,13:54:12.0
cccaEventText = ICM\acme\RouterA Node Manager started. Last shutdown was by operator
request.

```

The CCCA-Notifications.txt file is installed in the icm\snmp directory as part of Unified ICM/Unified CCE installation. It contains the complete set of SNMP notifications, which you can use to identify grouped events. The Correlation ID is the data used to generate the cccaEventComponentId, which is determined at run time. The following entries correspond to the SNMP notifications in the preceding example.

Table 3: Example: Raise Notification

Field	Value / Description
NOTIFICATION	1028105
cccaEventMessageId	2701295877 (0xA1028105)
DESCRIPTION	Node Manager on the ICM node has been given the command to stop ICM services. This occurs when an operator/administrator stops ICM services using ICM Service Control, 'nmstop', 'netstop', Control Panel Services, or shuts down the node.
cccaEventState	Raise
SUBSTITUTION STRING	The operator/administrator has shut down the ICM software on %1.
ACTION	Contact the operator/administrator to determine the reason for the shutdown.
cccaEventComponentId	{cccaEventOriginatingNode %1}
CorrelationId	{ CLASS_NM_INITIALIZING cccaEventOriginatingNode %1 }

Table 4: Example: Clear Notification

Field	Value / Description
NOTIFICATION	1028103
cccaEventMessageId	1627554051 (0x61028103)
DESCRIPTION	The Node Manager successfully started. The last reason the Node Manager stopped was because a clean shutdown of the ICM code was requested by the operator.
cccaEventState	Clear
SUBSTITUTION STRING	%1 Node Manager started. Last shutdown was by operator request.
ACTION	No action is required.
cccaEventComponentId	{ cccaEventOriginatingNode %1 }

Field	Value / Description
CorrelationId	{ CLASS_NM_INITIALIZING cccaEventOriginatingNode %1 }

Correlating Notifications

The `cccaEventComponentId` is the primary means of matching a clear event to a raise event. When a clear event is received, all pending raise events with the same alarm class and with a matching `cccaEventComponentId` should be cleared.

“Raise” Event:

`cccaEventComponentId:“4_1_acme-rgr_ICM\acme\RouterA”`

Event Class:CLASS_NM_INITIALIZING

`cccaEventState:raise(4)`

`cccaEventMessageId:2701295877`

`cccaEventSeverity:warning(2)`

`cccaEventText:The operator/administrator has shutdown the ICM software on ICM\acme\RouterA.`

“Clear” Event

`cccaEventComponentId:“4_1_acme-rgr_ICM\acme\RouterA”`

Event Class:CLASS_NM_INITIALIZING

`cccaEventState:clear(0)`

`cccaEventMessageId:1627554051`

`cccaEventSeverity:informational(1)`

`cccaEventText:ICM\acme\RouterA Node Manager started. Last shutdown was by operator request.`

Upon receipt of “Raise” event, categorize by severity

Upon receipt of “Clear” event, match to “Raise” using ‘`cccaEventComponentId`’

In the above example notifications, a simple string comparison of “” can suffice in matching the clear to the raise. `cccaEventComponentId` has the event class built into this value and the rest of the string was crafted to be sufficiently unique to ensure that the appropriate raises are cleared by the clear notification. (Remember: Multiple raise notifications can be cleared by a single clear notification.)

Sample logic:

If (`cccaEventState == “clear”`)

set ID = `cccaEventComponentId`;

for (all “raise” events where `cccaEventComponentId == ID`)

Acknowledge();

There is no one-to-one mapping of alarms by event message ID.



Note SNMP Notifications do not have a unique OID assigned to each alarm. The static assignment of an OID to a notification requires that that notification be explicitly documented (in Cisco customer-facing documents) and maintained following an established deprecation schedule. With so many Cisco devices in service, maintaining such a list is impossible. The event definition method in the CISCO-CONTACT-CENTER-APPS-MIB is consistent with the Cisco Unified Communications Manager (CISCO-CCM-MIB) and Cisco Unified Contact Center Express (CISCO-VOICE-APPS-MIB) product MIBs.

Single State Objects

A single state object has only a raise state. Because there is no corresponding clear event, the administrator must manually clear the object. Single state objects are typically used when a corresponding clear event cannot be tracked, for example the database is corrupt. Single state Unified ICM/Unified CCE SNMP notifications contain raise (9) value in the cccaEventState field.

The following example shows a value of Single-state Raise in the cccaEventState field to identify a single state object.

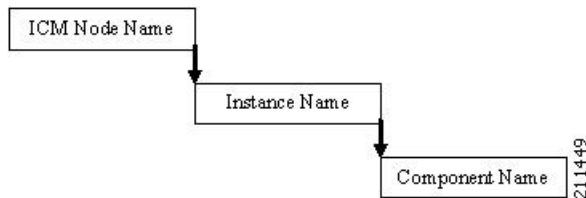
Table 5: Example "Single-State Raise" Notification

Field	Value / Description
NOTIFICATION	105023C
cccaEventMessageId	3775201852 (0xE105023C)
DESCRIPTION	The Router has detected that it is no longer synchronized with its partner. One result of this is that the Router might be routing some calls incorrectly.
cccaEventState	Single-state Raise
SUBSTITUTION STRING	The Router has detected that it is no longer synchronized with its partner.
ACTION	Action: Stop the Router on both sides. After both sides are completely stopped, restart both Routers. Alternate Action: Restart the Router on one side. After doing this, the Routers might still route some calls incorrectly, but they will be in sync. Other actions: Collect all rtr, mds, ccag process logs from both Routers from the entire day. Collect all sync*.sod files (where * is some number) that exist in the icm\ <instance>\ra .<="" a="" and="" b.="" contact="" directory="" icm\<instance>\rb="" in="" of="" router="" td="" the=""> </instance>\ra>
cccaEventComponentId	{ cccaEventOriginatingNode cccaEventOriginatingProcessName cccaEventOriginatingSide }
CorrelationId	{ CLASS_RTR_SYNC_CHECK cccaEventOriginatingNode cccaEventOriginatingProcessName cccaEventOriginatingSide }

Organizing SNMP Notifications

Using the contents of the following Unified ICM/Unified CCE SNMP notification fields, an SNMP Monitoring tool can group Unified ICM/Unified CCE SNMP notifications in an organized, hierarchical manner.

```
cccaEventOriginatingNode = CC-RGR1A\acme
cccaEventOriginatingNodeType = router(1)
cccaEventOriginatingSide = sideA(1)
```



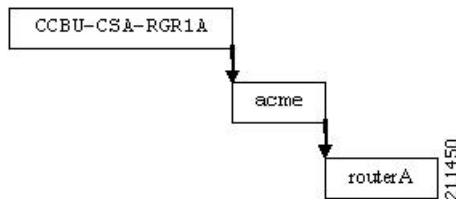
where:

Unified ICM/CCE Node Name = left side of cccaEventOriginatingNode

Instance Name = right side of cccaEventOriginatingNode

Component Name = cccaEventOriginatingNodeType + cccaEventOriginatingSide letter

For example:



Within this node, raise and clear events with the same cccaEventComponentId can be grouped as a single object.

CSFS Heartbeat Notification

The Customer Support Forwarding Service (CSFS) heartbeat notification should be monitored specifically as it is a critical SNMP notification.

Table 6: CSFS Heartbeat Notification

Field	Value / Description
NOTIFICATION	12A0003
cccaEventMessageId	1630142467 (0x612A0003)
DESCRIPTION	Periodic message to indicate MDS is in service and that the event stream is active.
cccaEventState	
SUBSTITUTION STRING	HeartBeat Event for %1

Field	Value / Description
ACTION	No action is required.
cccaEventComponentId	{ cccaEventOriginatingNode %1 }
CorrelationId	n/a



Note The CCCA-Notifications.txt file defines the decimal value of cccaEventMessageId for this event incorrectly as 19529731.

The heartbeat notification is sent periodically by the Logger CSFS process to indicate a healthy connection exists between the Router and the Logger, and that the Logger SNMP notification feed is active. The heartbeat interval is set to 720 minutes (12 hours) by default. The reason the interval is set this high is to accommodate using a modem to communicate notifications.

You can modify the interval via the Windows Registry value: heartbeatIntervalMinutes, in:

```
HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\\Logger<A or B>\CSFS\CurrentVersion
```

The interval can be as much as one minute longer than the configured interval, so the logic that reacts to these events should employ a certain “deadband” – in other words, allow for at least 60 seconds beyond the scheduled interval before assuming the worst.



Important Monitoring this heartbeat notification provides an additional measure of safety; if the communication infrastructure that sends notifications were to fail, one might assume that the system is operating, when in fact, it is not. If this heartbeat event ceases to arrive at the management station, this indicates that that communication infrastructure is impaired and immediately attention is necessary.



CHAPTER 4

Syslog Message Interface

- [The Cisco Log Message Format, on page 63](#)
- [Configure Syslog Destinations, on page 64](#)

The Cisco Log Message Format

The Cisco Log message format is:

```
<PRI>SEQNUM: HOST: MONTH DAY YEAR HOUR:MINUTES:SECONDS.MILLISECONDS TIMEZONE:  
%APPNAME-SEVERITY-MSGID:  
%TAGS: MESSAGE
```

An example of a CiscoLog formatted syslog event follows. An entry displays on a single line.

```
<134>25: host-w3k: Feb 13 2007 18:23:21.408 +0000: %ICM_Router_CallRouter-6-10500FF:  
[comp=Router-A][pname=rtr][iid=acme1][mid=10500FF][sev=info]: Side A rtr process is OK.
```

The following table describes the Cisco Log message fields:

Table 7: Cisco Log Message Fields

Field	Description
PRI	Encodes syslog message severity and syslog facility. Messages are sent to a single syslog facility (that is, RFC-3164 facilities local0 through local7). For more information, see RFC-3164.
SEQNUM	Number used to order messages in the time sequence order when multiple messages occur with the same time stamp by the same process. Sequence number begins at zero for the first message fired by a process since the last startup.
HOST	Fully qualified domain name (FQDN), hostname, or IP address of the originating system.
MONTH	Current month represented in MMM format (for example, “Jan” for January)
DAY	Current day represented in DD format. Range is 01 to 31.
YEAR	Current year represented in YYYY format.
HOURL	Hour of the timestamp as two digits in 24-hour format; range is 00 to 23.
MINUTE	Minute of the timestamp as two digits; range is 00 to 59.

Field	Description
SECOND	Second of the timestamp as two digits; range is 00 to 59.
MILLISECONDS	Milliseconds of the timestamp as three digits; range is 000 to 999.
TIMEZONE	Abbreviated time zone offset, set to +/-#### (+/- HHMM from GMT).
APPNAME	Name of the application that generated the event. APPNAME field values are: PRODUCT_COMPONENT_SUBCOMPONENT PRODUCT – such as ICM COMPONENT – such as Router SUBCOMPONENT – such as CallRouter
SEVERITY	Supported severity values are: 3 (Error) 4 (Warning) 6 (Informational) 7 (Debug)
MSGID	Hexadecimal message id that uniquely identifies the message, such as 10500FF.
TAGS	(Optional) Supported tags are: [comp=%s] - component name including side, such as Router-A [pname=%s] - process name, such as rtr [iid=%s] - instance name, such as acme1 [mid=%d] - message id, such as 10500FF [sev=%s] – severity, such as info
MESSAGE	A descriptive message about the event.

Configure Syslog Destinations

You can configure syslog destinations using the Cisco SNMP Agent Management Snap-in. The syslog feed is available only on the Unified ICM/Unified CCE Logger Node.

Before you begin

Before you configure the syslog destinations, start the syslog process (cw2kfeed.exe) from the Web Setup tool.

1. Open the Web Setup tool.
2. Select Component Management > Loggers, and then choose the instance of the logger for which you want to enable the syslog event feed.

3. In the Additional Options area, check the **Enable Syslog** check box to enable the syslog event feed process.

Figure 20: Enable Syslog

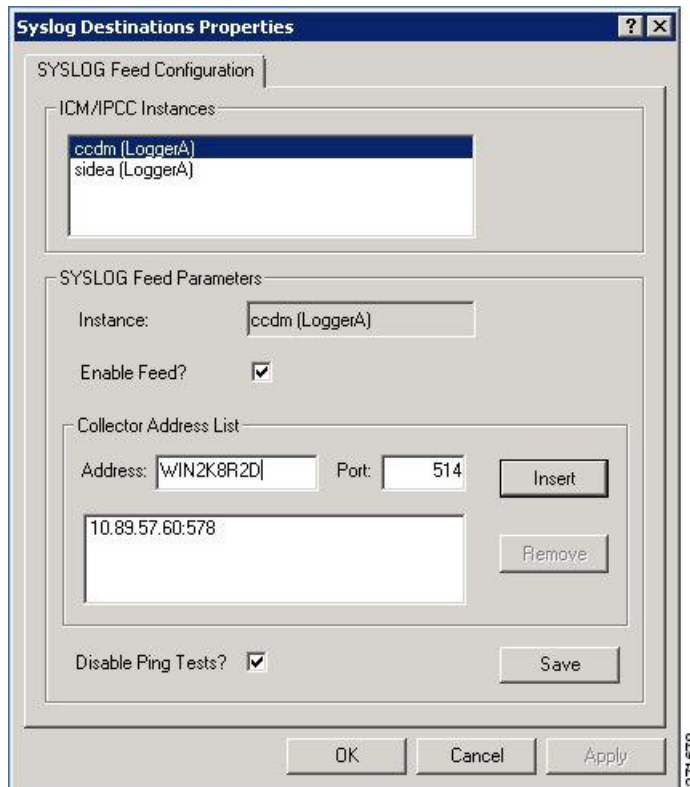


These steps runs the CW2KFEED process when the logger is started.

Procedure

- Step 1** Go to **Start** menu and select **Run**.
- Step 2** In the **Start** box, type **mmc / 32** and press Enter key.
- Step 3** Expand **Cisco SNMP Agent Management** in the left pane of MMC snap-in.
- Step 4** Highlight **Syslog Destinations** in the left pane under Cisco SNMP Agent Management. The following columns appear in the right pane:
 - ICM Instance Name
 - Feed Enabled
 - Ping Disabled
- Step 5** Right-click the white space in right pane and select **Properties**. A dialog box appears:

Figure 21: Syslog Destinations Properties Dialog Box



- Step 6** From the **ICM/IPCC Instances** list box, select one Unified ICM/Unified CCE instance. The **Instance** field displays the selected instance.
- Step 7** Check **Enable Feed?** check box.
- Step 8** In the **Collector Address** field, enter the IP address or Host Name.
- Step 9** (Optional) In the **Port** field, enter the collector port number on which syslog collector is listening.
- Note** The default port is 514.
- Step 10** Click **Insert** to add the IP address to the list.
- Note** You can add up to five IP addresses.
- Step 11** (Optional) To remove an existing IP address, select the IP address in the **Collector Address List** area, and click **Remove**.
- Step 12** (Optional) Check **Disable Ping Tests?** check box.
- Step 13** Click **Save**.
- Step 14** Click **OK**.



CHAPTER 5

Services and Processes

- [Services, on page 67](#)
- [Using the Local Desktop, on page 75](#)
- [ICM Service Control and Windows Task Manager, on page 75](#)
- [Using the Local Registry, on page 75](#)
- [Using the Remote SNMP Management Station, on page 76](#)

Services

The following table lists the processes running on a particular server. In the Description column, the criticality of a process is shown within brackets []. The key definitions are as follows:

Critical

This process is critical to the operation of the component. Failure of the process renders the application either dysfunctional or impaired.

Critical/Optional

This process is optional (needed for a feature often enabled via configuration or during product installation). However, if the feature is enabled, the process is critical and failure of the process is likely to render the application either dysfunctional or impaired.

Optional

This process is optional (needed for a feature often enabled via configuration or during product installation). Failure of the process is unfortunate but does not impair the Contact Center application.

Important

While failure of this process does not impair the Contact Center application, it disables an important capability.

Non-Critical

This process runs on the server under general operating conditions, but its failure has little or no impact on the Contact Center application.

An asterisk preceding the process name denotes that this process appears in the SNMP CISCO-CONTACT-CENTER-APPS-MIB `cccaComponentElmtTable`.

Table 8: Unified ICM/Unified CCE Processes

Component	Process	Description
Router	* router.exe	[Critical] This is the primary Router process.
	* rtsvr.exe	[Critical] Provides real-time data feed from the Router to the Administration & Data Server.
	* mdsproc.exe	[Critical] Message Delivery Service
	* ccagent.exe	[Critical] Router component that manages communication links between the Router and peripheral gateways.
	* dbagent.exe	[Critical] Manages connections and transactions (configuration updates) from configuration tools.
	* testsync.exe	[Non critical] Provides interface for component test tools.
	* appgw.exe	[Optional/Critical] The process that provides an interface for the Router to communicate with external applications.
	* dbworker.exe	[Optional/Critical] The process that provides the interface for the Router to query external databases.
	* [NIC].exe	<p>[Optional/Critical] A separate process is active for each Network Interface Controller (NIC) enabled during SETUP. The NIC process manages the interface to a telephony network.</p> <p>The presence of a NIC process in a Unified CCE deployment is very rare.</p> <p>NIC process names: atnnc.exe, cainnc.exe, netwrkcic.exe, crspnc.exe, gktmpnc.exe, incrpnc.exe, mcinnc.exe, gennnc.exe, ntnnc.exe, ntlnc.exe, sprnc.exe, ss7innnc.exe, stentornnc.exe, timnnc.exe, unisourcenc.exe</p>

Component	Process	Description
Logger	* configlogger.exe	[Critical] The process that manipulates configuration data.
	* histlogger.exe	[Critical] The process that inserts historical data into TMP historical tables in the Logger database.
	* recovery.exe	[Critical] This process bulk copies historical data from the TMP historical tables to the actual historical tables. Recovers and synchronizes historical data with its partner logger during failover if loggers are running duplex. It is also responsible for historical data purges in the Logger database based on configured retention parameters.
	* replication.exe	[Critical] The process that replicates data from the Logger to the Historical Data Server on an Administration & Data Server.
	* csfs.exe	[Critical] The alarm/event processor. CSFS distributes alarms/events send via EMS to supported alarm/event feeds, for example, SNMP, syslog. CSFS stands for Customer Support Forwarding Service, which in Unified ICM's infancy, forwarded events to a central monitoring location.
	* cw2kfeed.exe	[Optional] The syslog event feed. This process acquires events from the CSFS process, formats them appropriately in accordance with the syslog protocol and sends the events to the configured collector. If a syslog collector is not configured, the event feed from CSFS will not be processed.
	* campaignmanager.exe	[Optional/Critical] Outbound Option Campaign Manager. This process manages customer lists: provides customer records for every Dialer in the enterprise; determines when customers should be called again; maintains the "Do Not Call" list inmemory. The Campaign Manager also sends real time and historical data to the Router and distributes configuration information to Dialer and Import processes.
	* baimport.exe	

Component	Process	Description
		[Optional/Critical] Outbound Option Import process. This process imports contact lists into the Outbound Option database; applies query rules to the contact table to build dialing lists; determines the GMT value for each phone based on the region prefix configuration.
	sqlservr.exe	[Critical] Microsoft SQL server process
	sqlagent.exe	[Critical] Microsoft SQL server process

Component	Process	Description
PG	* opc.exe	[Critical] Open Peripheral Controller (OPC). This process acts as the brain for the peripheral gateway, including acting as a central collection and distribution point for all interaction with peripherals. OPC also ensures that all synchronization is accomplished with the other side. It also prepares and sends termination call detail (TCD) records as well as 5 minute and 30 minute reports.
	* mdsproc.exe	[Critical] Message Delivery Service
	* pgagent.exe	[Critical] MDS Peripheral Gateway component that manages the interface between the peripheral gateway and the central controller.
	* testsync.exe	[Non critical] Provides interface for component test tools.
	* eagtpim.exe	[Optional/Critical] The Cisco Unified CM peripheral interface manager process. This process manages the interface between OPC and the JTAPI Gateway. Multiple PIMs of the same type can be enabled for a PG. VRU PIMs and Unified CM PIMs may be coresident on a PG as well. This is very common in Unified CCE deployments but may not be present on all PGs. There may be multiple instances of this process running.
	* acmipim.exe	[Optional/Critical] The process is expected on the Unified SCCE Gateway PG – this Peripheral Interface Manager is responsible for the communication interface between the parent instance and the child instance.
	* vrupim.exe	[Optional/Critical] Peripheral Interface Manager process between OPC and a Voice Response Unit (VRU) or Interactive Voice Response (IVR). There may be multiple instances of this process running.
	* mrpim.exe	

Component	Process	Description
		<p>[Optional/Critical] The Media Routing Peripheral Interface Manager is the integration point for the Outbound Option Dialer, Cisco Email Manager (CEM), Cisco Collaboration Server (CCS) and the Enterprise Chat and Email.</p> <p>There may be multiple instances of this process running.</p>
	* msgis.exe	<p>[Optional/Critical] Message Integration Service (MIS), which provides a mechanism to share call context data with a VRU. This process is only present on a PG with a VRU PIM.</p>
	* ctiosservernode.exe	<p>[Critical] The CTI OS Server process that manages connections from CTI clients (agent desktops), retains (real-time) data about agents and acts as the conduit for events and control messaging between CTI Server and CTI clients.</p>
	* jtapigw.exe	<p>[Critical] JTAPI Gateway that manages the interface to the Unified Communications Manager IP PBX via the JTAPI client to the CTI Manager on the Unified CM. On the other side, the JTAPI Gateway connects to the Unified CM PIM and translates JTAPI messages and events into a format expected by the PIM.</p>
	* ctisvr.exe	<p>[Critical] CTI Gateway (CTI Server) process that processes (GED-188) messages between CTI OS and OPC.</p> <p>Note: In legacy implementations, CTI Server manages connections to CTI desktops.</p>

Component	Process	Description
Administration & Data Server (AW/HDS)	* configlogger.exe	[Critical] Processes inbound configuration data.
	* updateaw.exe	[Critical] Updates the local configuration database with configuration data from the central controller.
	* rtclient.exe	[Critical] Receives a real-time data feed (from a real-time distributor) and updates the local database.
	* rtdist.exe	[Critical] Manages inbound real-time data from the real time server on the Router and distributes it to real-time clients.
	* replication.exe	[Critical] Manages replicated historical data received from the Logger (HDS only) and inserts historical data in the HDS database. In addition, it is responsible for historical data purges in the HDS database based upon configured retention parameters.
	* cmsnode.exe	<p>[Optional] Configuration Management System (CMS). Manages configuration data for the ConAPI interface. This is a necessary interface (process) for the System CCE web configuration. Thus, for System Unified CCE, this is an important process. Also, if the customer has purchased the Cisco Unified Contact Center Management Portal (Unified CCMP), CONAPI is also used. However, for a Unified CCE deployment without Unified CCMP, this process is not critical.</p> <p>In a recent version of Unified CCE, cmsnode.exe runs by default but it is difficult for a management station to know whether it is necessary. Therefore, this is listed as Optional.</p>
* cms_jserver.exe	<p>[Optional] Configuration Management System (CMS) Jaguar Server. This process works with cmsnode.exe for CMS to provide Java interfaces for ConAPI.</p> <p>In a recent version of Unified CCE, cms_jserver.exe runs by default but it is difficult for a management station to know whether it is necessary. Therefore, this is listed as Optional.</p>	

Component	Process	Description
	tomcat<version>.exe	[Optional/Critical] Apache Tomcat servlet engine for SCCE web config.
	* iseman.exe	[Optional] Internet Script Editor
	sqlservr.exe	[Critical] Microsoft SQL server process
	sqlagent.exe	[Optional] Microsoft SQL server process
All Nodes	nodeman.exe	[Critical] Node Manager. This process monitors the status of all Unified ICM/Unified CCE processes on the server; should a process terminate unexpectedly, the Node Manager automatically restarts that process.
	nmm.exe	[Critical] Node Manager Manager. This process monitors the primary Node Manager (nodeman.exe) process; should the primary Node Manager (nodeman.exe) process terminate unexpectedly, the Node Manager Manager restarts it.
	snmpdm.exe	[Important] SNMP primary agent.
	cccsnmpgmt.exe	[Important] SNMP agent management service – this service manages the SNMP agent infrastructure and restarts any agents that may terminate unexpectedly. It also ensures that the agent processes run at a reduced priority so as to not adversely impact server performance.
	msnsagt.exe	[Important] Microsoft built-in subagent adapter.
	UcceSnmpHelperX86.exe	[Important] Used by hostagt.exe and cccaagent.exe to get information about 32-bit processes that are currently running on the machine.
	hostagt.exe	[Important] HOST-RESOURCES-MIB subagent.
	sappagt.exe	[Important] SYSAPPL-MIB subagent.
	cccaagent.exe	[Important] CISCO-CONTACT-CENTER-APPS-MIB subagent.

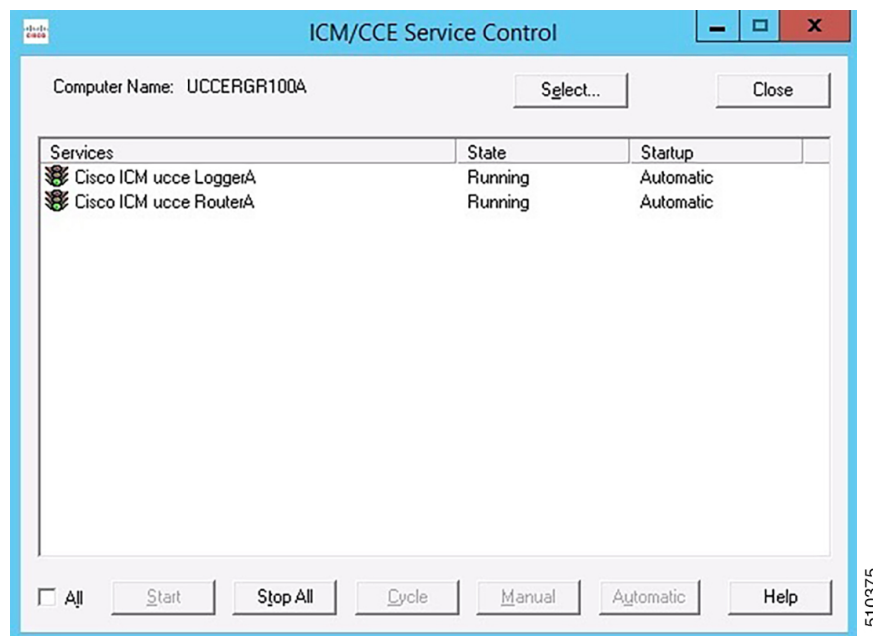
Using the Local Desktop

Use the Unified ICM Service Control and the local registry to monitor Unified ICM/Unified CCE components and their processes.

ICM Service Control and Windows Task Manager

The Unified ICM Service Control displays the Node Manager service for each Unified ICM/Unified CCE component and its state and startup settings. Each Node Manager service appears in the following format: Cisco ICM <instance> <component>. The following Unified ICM Service Control window example lists information about the Node Manager services running on the local machine. The Router component Node Manager service is identified as “Cisco ICM acme RouterA”.

Figure 22: ICM Service Control



You can no longer view Unified ICM/Unified CCE processes on the Application tab of Windows Task Manager. To view the status of each process, use the Diagnostic Framework Portico. For more information, see [Accessing the Diagnostic Framework Through the Built-In User Interface \(Portico\)](#), on page 188.

Using the Local Registry

The Unified ICM/CCE Windows registry hive contains the set of all installed components and their processes. However, to determine which processes are being managed, traverse the Node Manager registry key for each component.

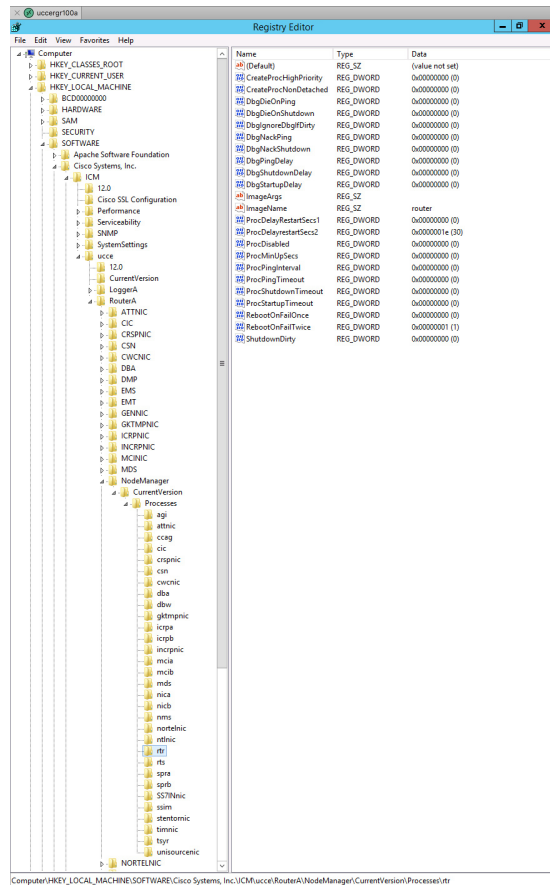
The following illustration shows the set of processes associated with the Cisco ICM acme RouterA component. The key name for the Router process is rtr; it appears highlighted in the navigation pane of the Registry Editor

window. The process name, Router, is contained in the ImageName value; it appears without the .exe file extension. If the ProcDisabled value is set to 0—as is the case for the Router process—the RouterA Node Manager process starts and manages the process.



Note The key name is typically not the same as the process name.

Figure 23: Registry Editor



510374

Using the Remote SNMP Management Station

In addition to the information available using the local desktop tools and registry, the Contact Center SNMP agent returns information about all Unified ICM/Unified CCE-enabled processes regardless of whether they are running. This information is available from the `cccaInstanceTable`, `cccaComponentTable`, and `cccaComponentElmtTable`. The instance number and component index correlate a process to a specific instance and component.

The first example shows the entries for acme-RouterA Router process. The `cccaComponentElmtRunID` value, which is the process ID, is valid if the `cccaComponentElmtStatus` is active, started, or standby.

```
cccaInstanceName.0 = acme
cccaComponentType.0.1 = router(1)
```

```
cccaComponentName.0.1 = RouterA
cccaComponentStatus.0.1 = started(4)
cccaComponentElmtName.0.1.5 = router
cccaComponentElmtRunID.0.1.5 = 4040
cccaComponentElmtStatus.0.1.5 = active(5)
```

The next example shows the entries for acme-LoggerA, the configlogger process. The `cccaComponentElmtRunID` value, which is the process ID, is valid if the `cccaComponentElmtStatus` is not stopped (3).

```
cccaInstanceName.0 = acme
cccaComponentType.0.2 = logger(2)
cccaComponentName.0.2 = LoggerA
cccaComponentStatus.0.2 = stopped(3)
cccaComponentElmtName.0.2.8 = configlogger
cccaComponentElmtRunID.0.2.8 = 0
cccaComponentElmtStatus.0.2.5 = stopped(3)
```




CHAPTER 6

Contact Center Trace Levels

- [Trace Levels, on page 79](#)
- [EMS Log Compression, on page 86](#)
- [Set Router Tracing, on page 87](#)
- [How to Set OPC Tracing, on page 88](#)
- [How to Set Unified CCM PIM Tracing, on page 90](#)
- [How to Set JTAPI Gateway Tracing, on page 90](#)
- [How to Set Contact Sharing Tracing, on page 91](#)
- [How to Set CTI Server Tracing, on page 91](#)
- [Setting CTI OS Tracing, on page 92](#)
- [Setting VRU PIM Tracing, on page 92](#)
- [Setting Outbound Option Tracing, on page 93](#)
- [Trace File Retention Settings, on page 94](#)
- [Router Full Dump Enabled by Default, on page 95](#)

Trace Levels

Support personnel who debug the Unified Communication solution need not know the details of trace levels across Unified Communication solution applications. If debugging a problem requires more detailed debug information, three levels of trace setting exist that can map internally to a particular application or application component. The intent is not to revamp existing trace setting values but to map the levels to the relevant and existing trace settings for a particular component. Use the following defined trace levels with the Diagnostic Framework Portico and the Unified System CLI tools.

The following trace levels are defined for the Unified Communication solution:

Trace Level	Trace Value	Description
Default	0	Default install, should have no or minimal performance impact
Warning	1	Log more detailed (plus default level) trace messages, small performance impact
Error	2	Log more detailed (plus warning and default level) trace messages, medium performance impact
Debug	3	Log most detailed (plus error and warning and default level) trace messages, high performance impact.



Note If you have enabled the debug trace levels, disable them after collecting the logs to avoid an unnecessary performance impact to your solution.

If the trace level does not match any of the defined levels, it displays custom (99).

Most EMSTraceMasks are based on this registry key: `HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<Instance>\<Component>\EMS\CurrentVersion\Library\Processes\<process>\EMSTraceMask`

Get and Set trace level and collect trace files are supported only for the following processes.



Note If the trace mask is the same for multiple levels, the GetTraceLevel returns the highest level. For example, GetTraceLevel returns Level 3 for Logger/baimport.

Trace-All Nodes

You can set trace levels on these processes:

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
NM	0x00	0x0F	0x0F	0xFF
NMM	0x00	0x0F	0x0F	0xFF

The Diagnostic Framework does not support the Administrator Workstation.

Trace-Administration and Data Server

You can set trace levels on these processes for the Administration and Data Server:

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
CONFIGLOGGER	0x00	0x0F	0xFF	0xFFF
CMSNODE	0x00	0x00	0x00	0xFFFFFFFF
CMS_JSERVER	0x00	0x00	0x00	0xFFFFFFFF
REPLICATION	0x00	0x0F	0xFF	0xFFF
RTCLIENT	0x00	0x0F	0xFF	0xFFF
RTDIST	0x00	0x0F	0xFF	0xFFF
UPDATEAW	0x00	0x0F	0xFF	0xFFF

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
ISEMAN	0x00	0x00	0x00	0x01



Note The minimum and default trace level for the CMS, CMSJServer and ISE components is 2.

Trace-Router

You can set trace levels on these processes for the Router:

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)	Notes
Agi	0x00	0x01	0x07	0x3F	—
ccagent	0x00	0x03	0x0F	0xFF	—
dbagent	0x00	0x01	0xFF	0xFF	—
DBWORKER	0x00	0x01	0xFF	0xFF	—
mdsproc	0x00	0x07	0xFF	0xFF	—
rtr	0x00	0x0F	0xFF	0xFFF	—
ROUTER *	Route Requests	Route Requests	- Network VRU - Trans Route - VRU Bank - CIC Request - Script Select	- Call Queuing - Agent changes - Call Type Real Time	In case of RTRTRACE or RTRTEST Note: If you restart the Router process, the settings return to the default level.

Trace-Logger

You can set trace levels on these processes for the Logger:

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3(Debug)
BAIMPORT	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3(Debug)
CAMPAIGN MANAGER	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF
CONFIGLOGGER	0x00	0x0F	0xFF	0xFFF
CSFS	0x00	0x00	0x00	0xFF
CW2KFEED	0x00	0x00	0x00	0x07
DTP	0x00	0x04	0x06	0x0F
HISTLOGGER	0x00	0x0F	0xFFF	0xFFF
RECOVERY	0x00	0x0F	0xFFF	0xFFF
REPLICATION	0x00	0x0F	0xFFF	0xFFF

Trace-Peripheral Gateway

You can set trace levels on these processes for the PG:

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
JTAPIGW *	JT_JTAPI_EVENT_USED JT_TPREQUESTS JT_PIM_EVENT JT_ROUTE_MESSAGE	JT_CONNECTION *CONF*	JT_JTAPI* JT_HEX JT_ROUTE* JT_TERM* JT_LOW*	JT*
MDSPROC	0x00	0x07	0x0F	0xFF
MSGIS	0x00	0x00	0x00	0x3F
OPC **	Default, cstacerEMSTraceMask = 0x40	agent, incrmgs, closedcalls, tpmsg, routingEMSTraceMask = 0x40 Note: Remove "default" tracing set in Default(0) level, but include cstacer.	Calls, NCT, simplified EMSTraceMask = 0x40 Note: Remove "default" tracing set in Default(0) level, but include Level 1.	Missingdata, halfhour EMSTraceMask = 0x40 Note: Remove "default" tracing set in Default(0) level, but include Level 2.
PGAGENT	0x00	0x03	0x0F	0xFF

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
EAGTPIM *	tp* precall *event csta* call_object teld_agent_state opcrequest	periph* jtapi_dialed*	autoconfig* teld* call_match_timing timer*	lock* universal* service* threadid jtapi*
VRUPIM	EMSTraceMask= 0x0 EMSUserData= 0x71f7e0	EMSTraceMask= 0x0 EMSUserData= 0x71f7e0 00000000000000000000 00000000000000000000 00000000000000000000 00000000000000000000 00000000000000000000	EMSTraceMask= 0x0 EMSUserData= 0x71f7e0 00000000000000000000 00000000000000000000 00000000000000000000 00000000000000000000 00000000000000000000	EMSTraceMask= 0x0EMSUserData= 0xf1fff0 00000000000000000000 00000000000000000000 00000000000000000000 00000000000000000000 00000000000000000000
ACMIPIM	EMSUserData = (hex) 01, 7f, 46, 00, 00, 00, 00, 00, 00, 00, 00, 01, 00, 00, 00, 00, 00, 3f, ff, ff, ff, 67, cf, d7, fd, ef, ff, ff, ff, ff, ff, ff, ff, ff, ff, f0, fa For reference, this is the default + all_peripherals	EMSUserData = (hex) f5, 7f, 46, 00, 00, 00, 00, 00, 00, 00, 00, 01, 00, 00, 00, 00, 00, 3f, ff, ff, ff, 67, cf, d7, fd, ef, ff, ff, ff, ff, ff, ff, ff, ff, ff, f0, fa For reference this is level 0 + timer events	EMSUserData = (hex) f5, 7f, c6, 00, 00, 00, 00, 00, 00, 00, 00, 01, 00, 00, 00, 00, 00, 3f, ff, ff, ff, 67, cf, d7, fd, ef, ff, ff, ff, ff, ff, ff, ff, ff, ff, f0, fa For reference this is level 1 + Monitor Item traversal	EMSUserData = (hex) f5, 7f, f6, 00, 00, 00, 00, 01, ff, ff, fe, c1, 00, 00, 00, 00, 00, 3f, ff, ff, ff, 67, cf, df, fd, ef, ff, ff, ff, ff, ff, ff, ff, ff, ff, ff, fe For reference this is level 2 + locks + socket data
ARSPIM *	tp* precall *event csta* call_object teld_agent_state opcrequest	periph*	autoconfig* teld* call_match_timing timer*	lock* universal* service* threadid
MRPIM	EMSUserData = 0x00 Procmon: > trace mr* /off Note Level 2 is the default level for MRPIM.	EMSUserData = 0x40 Procmon: > trace mr* /off > trace mr_msg_comm_session /on	EMSUserData = 0x58 Procmon: > trace mr* /off > trace mr_msg_comm_session/on > trace mr_*_mr /on	EMSUserData = 0x5F Procmon: > trace mr* /off > trace mr_msg_comm_session/on > trace mr_*_mr /on > trace mr_*_inrc /on > trace mr_*_csta /on
Avaya Aura PIM (Symposium)	Default	Default	Default	Tpcsta*, call*, csta*
AAS	Default	EMS_TRACE_GENERAL	EMS_TRACE_CONAPI EMS_TRACE_SEI	EMS_TRACE_AASDRIVER EMS_TRACE_MSL
Aspect PIM	Default	Default	Default	Tpcsta*, call*, csta*, app*, pim*, rtb*

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
Avaya ECSPIM	Default	Default	Default	Bri*, agent*, call*, csta*, cms*, tp*, 3pdc*, route*, cv*
Avaya TAESPIM	Default	Default	Default	agent*, call*, csta*, cms*, tp*, monitor*, route*, value*, tsapi*
CTISRV	0x000000f0	0x000000f6	0x000000fe	0x000000ff
CTIOS SERVER NODE	0x00060A0F	0x00240A2F	0x00260A2F	0x002E0A2F
BADIALER	EMSTraceMask= 0x0000003f EMSUserData= 0xFFFF	EMSTraceMask= 0x0000003f EMSUserData= 0xFFFF	EMSTraceMask= 0x0000007f EMSUserData= 0xFFFF	EMSTraceMask= 0x0000007f EMSUserData= 0xFFFF

Trace-Web Setup

You can set trace levels on the Web Setup process.

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
Web Setup	EMERGENCY	CRITICAL	WARNING	DEBUG

Websetup uses log4j.net for logging. Websetup uses a XML file (log4j.xml) through which you can set the trace levels. The XML file also contains other information you require for logging.

You can find the log4j.xml file here: <InstallDrive>\icm\tomcat\webapps\setup\WEB-INF\classes\log4j.xml

Trace-Diagnostic Framework

You can set trace levels on the Diagnostic Framework.

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)	Notes
Diagnostic Framework	Info	Info	Info	Debug	

When the Diagnostic Framework receives a request for its own trace level, if the trace level is at Info, Level 2 is returned. When the Diagnostic Framework receives a request to be set for Level 0, Level 1, or Level 2, the trace level is set to Info.

Trace–SADLib

You can set trace levels on SADLib.

Process	Trace Level	Trace Value	Description
SADLib	0	NO	No logs are generated.
	1	WARNING	The Warning and Error logs are generated.
	2	INFO	The Warning, Error, and Info logs are generated.
	3	DEBUG	The Warning, Error, Info, and Debug logs are generated.

Reference Tables

Regarding JTAPI logging,

Jtapi uses EMSUserData value default (OX49E2) to control logging, we can enable/disable JT_ bits using procmon (trace command). JT_ maps to below tables values which is masked with EMSUserData to control tracing.

Process	Level 0 (Default - Error)
JT_HEARTBEATS	1
JT_TPREQUESTS	2
JT_HEX	3
JT_JTAPI*	4-7
JT_CONNECTION	8
JT_PIM_EVENT	10
JT_ROUTE*	11-12
JT_LOW_LEVEL*	13-14
JT_CONF_XFER	15
JT_TERM_EVENT RTP	16
JT_DEBUG	17

Regarding MRPIM logging

Similar to jtapi, mrpim default EMSUserData is 0xD8, we can enable/disable mr* bit using procmon(trace command)

Process	Level 0 (Default - Error)
mr_msg_config	1
mr_msg_comm_session	2
mr_heartbeat_messages	3
mr_msg_incoming_mr	4-7
mr_msg_outgoing_mr	8
mr_msg_incoming_inrc	10
mr_msg_outgoing_inrc	11-12
mr_msg_outgoing_csta	13-14
mr_function_call	15
mr_outgoing_opc	16

EMS Log Compression

To collect logs that span a greater period of time, EMS log files from the CTI OS Server and the following PG components are zipped:

- Router
- OPC-CCE
- OPC-TDM
- CTISVR
- EAGTPIM
- JTAPIGATEWAY
- VRUPIM
- BADIALER
- MRPIM
- CTI OS Server



Note These are the only components that currently support EMS log compression.

Dumplog

Dumplog handles the compressed EMS files and can be used in the general way. Dumplog looks for gzip.exe in <Install Drive>\icm\bin to unzip compressed EMS files before dumping logs. To dump logs from compressed EMS files (with .gz extension) outside of a PG or CTI OS Server, unzip the EMS files before you use dumplog.

EMS File Compression Control

Use the EMSZipCompressionEnabled registry key in \EMS\CurrentVersion\Library\Processes\<<process name> to enable or disable compression of EMS log files. Do not modify this registry key. This key takes effect only on components that support EMS file compression.

Other Registry Keys

The following two other registry keys are also available in
...\EMS\CurrentVersion\Library\Processes\<<node name>

EMSZipFormat
EMSZipExtension



Note Do not modify these registry keys.

Set Router Tracing

To set the Unified ICM/CCE Router, use the Router Trace utility. This utility is a single-form Windows GUI utility that is loaded on the Unified ICM/Unified CCE server.



Note The router process must be running before you set router tracing or attempt to retrieve router traces. This requirement applies to any tool which sets or retrieves router tracing, including, for example, RTTEST, RTRTRACE, and System CLI. (The router process must be running because the router trace settings are only stored in memory).



Note Business Hours tracing has to be set or reset using RTR Trace utility or RTTEST utility only. Setting the trace level for Router in Diagnostic portico will not change the Business Hours setting.

All trace settings using “RTRTRACE” take effect immediately in the Router.

You can observe specific status of call routing, call type, skill group, and schedule target variables using the following RTTEST command: `rttest /cust <instance>/node <node>`.

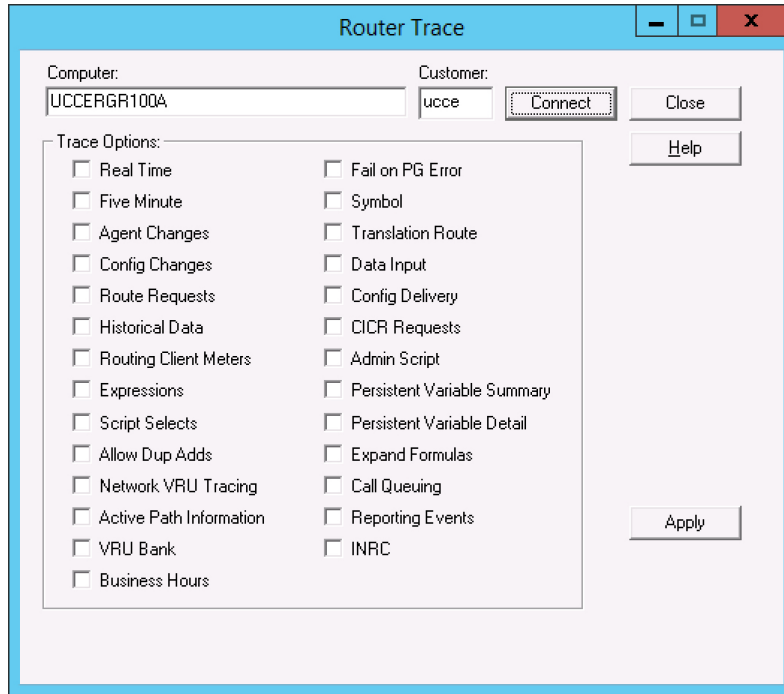
You can monitor a particular variable and determine if its value is incremented or decremented by enabling the RTTEST “watch” command on router logs: `rttest: watch <variable>`.

The logs are written only when value is changed.

Procedure

- Step 1** Connect to server through remote desktop or go to local console.
- Step 2** Run command `C:> \icm\bin\rtrtrace` to invoke RTRTRACE from ICM\BIN

Figure 24: Router Trace Utility



Step 3 Set trace options.

When a call routing failure occurs, the basic traces should at the minimum be “Route Requests” and “Translation Route” if you use translation routing.

Also, enable the other tracing depending on the specific problems you see.

For...	Enable...
Any type of VRU	Network VRU Tracing
NAM-CICM (Hosted)	CICR Requests
Suspected queuing issues	Call Queuing
Reporting events problems	Reporting Events
Agent issues	Agent Changes
Business Hours problems	Business Hours

How to Set OPC Tracing

To set Unified ICM/Unified CCE OPC tracing, use the OPCTEST utility. This is a command-line utility and you require remote desktop or local console access.

Command Syntax (launch):

```
C:> opctest /cust <instance> /node <node>
```

Where <instance> is the Unified ICM/Unified CCE instance name and <node> is the desired node name (for example, /cust cust1 /node PG1A).

After you invoke the instance name, you are presented with an opctest: prompt where you can enter commands according to the syntax expected. To display all commands, enter a “?” at the opctest: prompt. However, OPCTEST is a powerful utility and if you use it incorrectly, it can have a negative effect on a production system in operation. Do not run a command against a production system unless you are absolutely certain of the impact it can introduce.

Use the following commands to alter default trace levels. Before using the commands, understand your current utilization to ensure there is sufficient capacity to accommodate the added tracing.

General Diagnostics

```
opctest:debug /on
```

Diagnosing Network Transfer Issues

```
opctest:debug /on
opctest:debug /NCT
```



Note Dialog ID in network transfer call flows appear as a negative number in OPC logs. This is applicable for other components like Router and VRU PIM as well. This is to ensure that Router generated DialogID's do not conflict with DialogID's originated from the pre-routing client (also referred to as NIC DialogID). This pre-routing client can either be a NIC or a VRU PIM integrated with CVP. While the router-assigned DialogID can be any unique number with the most significant bit set, the router will use the expired NIC DialogID value as a troubleshooting aid.

Diagnosing Multimedia Issues

```
opctest:debug /on

opctest:debug /task /passthru
```

Diagnosing VRU PG Issues

```
opctest:debug /on
opctest:debug /passthru
```

The default is:

```
opctest:debug /routing /agent /closedcalls /cstacer /rcmsg /tpmsg /simplified /inrcmsg
and
```

```
EMSTracemask = 0x40
```

EMSTracemask is reset in the Windows registry.

TAC directs you to alter or add additional tracing based upon the analysis of collected logs.

How to Restore Default Trace Levels

```
opctest:debug /on
```

This parameter turns on the /default tracing, modifies the EMSTracemask to 0x40, and turns off all other enabled tracing.

How to Display Trace Levels

```
opctest:debug /showtrace
```

This parameter displays current trace levels enabled on the peripheral.

How to Set Unified CCM PIM Tracing

To reset trace levels with the Unified Communications Manager Peripheral Interface Manager component (for example, “EAGTPIM”), use the ProcMon (process monitoring) utility. This is a command-line utility and you require remote desktop or local console access.

Table 9: Setting Unified CCM PIM Tracing

Command Syntax (launch)	C:> ProcMon <instance> <node> pim<pim number>
Example	C:> ProcMon acme PG1A pim1
Commands	>>>>debug /on

How to Set JTAPI Gateway Tracing

To reset trace levels for the Unified Contact Center JTAPI (Java Telephony Applications Programming Interface) Gateway component (for example, “JTAPIGW”), use the ProcMon (process monitoring) utility. This is a command-line utility and you require remote desktop or local console access.

Table 10: Setting JTAPI Gateway Tracing

Command Syntax (launch)	C:> ProcMon <instance> <node> jgw<jtapigw number>
Example	C:> ProcMon acme PG1A jgw1
Commands	>>>>trace* /off >>>>debug /on

How to Set JTAPI Gateway Default Tracing

The default tracing for JTAPI gateway consists of a set of tracing levels that currently exist.

To enable only the default tracing, enter the following commands in ProcMon:

trace * /off

Note: debug /on does not turn off non-default tracing so you need this first.

debug /on This enables only default tracing.

To turn off debug tracing, enter the following command in ProcMon:

debug /off This turns off only default tracing. All other tracing is not affected.

How to Set Contact Sharing Tracing

The Contact Sharing service is an optional process which runs under the main Router service (when enabled through web setup on an Contact Director deployment). Tracing levels for this process are set through a ProcMon connection as detailed in the following table.

Table 11: Setting Contact Sharing Tracing

Command Syntax (launch)	C:>ProcMon <customer name> <ra or rb> <csn> <systemname>
Example	C:\>ProcMon bos01 ra csn boston-p-cc
Commands	>>>trace <bit> /on >>>trace <bit> /off



Note "ra" and "rb" = Router A or B
"csn" = Contact Sharing Node

How to Set CTI Server Tracing

To reset trace levels with the Unified ICM/Unified CCE CTI Server (for example, CTI Gateway or CG), use the Microsoft Registry Editor (regedit) to modify the trace mask saved in the Windows registry.

Table 12: Setting CTI Server Tracing

Registry Key	HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\<CG#A/B>\EMS\CurrentVersion\Library\Processes\ctisvr
Example	HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\acme\CG1A\EMS\CurrentVersion\Library\Processes\ctisvr
Item	EMSTraceMask
Value	F0 (hex) This is the default value. The value of F0 provides sufficient tracing information to troubleshoot most issues.

Setting CTI Server Default Tracing

The default tracing level for CTI Server is EMSTraceMask = 0xF0. Do not enable any other tracing at the default trace level. EMSUserData should be NULL.

ProcMon debug commands:

debug /on sets the EMSTraceMask to the default value of 0xF0 and NULL out EMSUserData. No other command is needed to set default tracing.

debug /off sets EMSTraceMask to 0x00 and NULL out EMSUserData.

Setting CTI OS Tracing

Resetting trace levels with the Unified ICM/Unified CCE Cisco Computer Telephony Integration Option (CTI OS) is accomplished by altering the trace mask saved in the Windows registry. Use the Windows REGEDIT utility to change this numeric value.

Table 13: Setting CTI Server Tracing

Registry Key	HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\ <instance>\ctios\ems\currentversion\library\processes\ctios< td=""> </instance>\ctios\ems\currentversion\library\processes\ctios<>
Example	HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\acme\CTIOS\EMS\CurrentVersion\Library\Processes\ctios
Item	EMSTraceMask
Value	60A0F (hex) Increasing the trace levels (other than the Default 0x00060A0F) impacts the CTI OS Server performance. You must revert High Tracemask to the default trace levels after collecting the required logs.
Levels	Level 0: 0x00060A0F Level 1: 0x00240A2F Level 2: 0x00260A2F Level 3: 0x002E0A2F

Setting VRU PIM Tracing

Resetting trace levels with the Unified ICM/Unified CCE VRU Peripheral Interface Manager (PIM) is accomplished by altering the trace mask and user data values saved in the Windows registry. Use the Windows REGEDIT utility to change these numeric values.

Table 14: Setting VRU PIM Tracing

Registry Key	HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\ <instance>\pg<pg b>\ems\currentversion\library\processes\pim<pim="" number><="" number>\a="" or="" td=""> </instance>\pg<pg>
Example	HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\acme\PG2A\EMS\CurrentVersion\Library\Processes\pim1

Item	EMSUserData
Value	7F F7 E0 (hex)
Item	EMSTraceMask
Value	0 (zero)

When you collect the trace logs, collect both VRU PIM trace logs and the VRU trace capture file. To obtain VRU trace capture files, run the VRUTRACE tool in the following directory:

```
\icm\

```

For example: \icm\acme\pg2a\vrucap

Setting VRU PIM Default Tracing

The default tracing for VRU PIM consists of a set of tracing levels that currently exist.

ProcMon debug commands:

debug /off turns off all tracing

debug /on enables default tracing only and turns off any previously enabled tracing

Setting Outbound Option Tracing

The utility tools provide centralized control to set up each component trace level. Additionally, you can manually modify the registry key values.

How to Reset CampaignManager Tracing

To reset CampaignManager trace levels, use the Microsoft Registry Editor (regedit) to modify the trace mask saved in the Windows registry.

Registry Key:

```
HKLM\SOFTWARE\Cisco Systems,  
Inc.\ICM\

```

Example:

```
HKLM\SOFTWARE\Cisco Systems,  
Inc.\ICM\m3pc1\LoggerA\EMS\CurrentVersion\Library\Processes\CampaignManager
```

How to Reset balImport Tracing

To reset balImport trace levels, use the Microsoft Registry Editor (regedit) to modify the trace mask saved in the Windows registry.

Registry Key:

```
HKLM\SOFTWARE\Cisco Systems,
Inc.\ICM<instance>\LoggerA\EMS\CurrentVersion\Library\Processes\baImport
```

Example:

```
HKLM\SOFTWARE\Cisco Systems,
Inc.\ICM\m3pc1\LoggerA\EMS\CurrentVersion\Library\Processes\baImport
```

How to Reset Dialer Tracing

To reset Dialer trace levels, use the Microsoft Registry Editor (regedit) to modify the trace mask saved in the Windows registry.

Registry Key:

```
HKLM\SOFTWARE\Cisco Systems,
Inc.\ICM<instance>\Dialer\EMS\CurrentVersion\Library\Processes\baDialer
```

Example:

```
HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\m3pc1\Dialer\EMS\CurrentVersion\Library\Processes\baDialer
```

Trace File Retention Settings

You can modify several Windows registry values to adjust the trace log retention parameters, for example, increase the amount of trace data – extend the trace retention window. To modify the trace log parameters, use the Microsoft Registry Editor (regedit).

Unified ICM/Unified CCE Event Management System (EMS) tracing is stored in a binary format in a set of files in a directory on the local drive following a specific structure.

Trace log file location

```
[Drive]:\icm<instance>\<node>\logfiles
```

Example

```
C:\icm\acme\pg1a\logfiles
```

Trace log file names

```
Process_YYMMDD_HHMMSS.ems
```

Example

```
opc_090713_123025.ems
```

This is an OPC trace log file that was created 13 July, 2009 at 12:30:25.

Under the control of the Event Management System, the following rules apply while traces are written to the trace log files:

- If the size of this file is greater than or equal to the maximum (configured) size that a single EMS trace log file is allowed, the file is closed and a new file is created.
- If the maximum number of trace log files for this process is greater than the maximum (configured) number of trace log files, then the oldest trace log file is deleted.
- If the total combined size of all process trace log files is greater than or equal to the maximum (configured) total size of all process trace log files, then the oldest trace log files are deleted until the total size is less than the configured maximum size.

Registry Items

You can change the following registry item values to increase or decrease the amount of disk space allocated for a single process.

Registry key

```
HKLM\SOFTWARE\Cisco Systems,
Inc.\ICM\

```

Example

```
HKLM\SOFTWARE\Cisco Systems,
Inc.\ICM\acme\PG1A\EMS\CurrentVersion\Library\ Processes\opc
```

Items

EMSLogFileMax

The maximum size, in bytes, of a single trace log file for this process.

EMSLogFileCountMax

The maximum number of trace log files permitted for this process.

EMSAIILogFilesMax

The total space allowed for all trace log files (combined size) for this process.



Note EMSLogFileMax multiplied by EMSLogFileCountMax may be greater than EMSAIILogFilesMax and it often is by default; this is to ensure trace log files created by frequent process restarts (where a number of small trace log files are created) are not lost when the max count is exceeded but very little disk space is used. EMSAIILogFilesMax is used to guarantee that under any circumstances, the maximum amount of disk space allocated is never exceeded.

The default values of these items are evaluated with every release of the Unified ICM/Unified CCE to determine the optimal limits based on disk usage of the application and typical disk capacity of servers available at the time of release. In nearly all cases, the default values are increased over time as disk drive sizes increase.

Router Full Dump Enabled by Default

In Release 10.0(1), router full dump is enabled by default. This change to the default setting is intended to provide more information to help troubleshoot the issue if a critical process crashes.

The registry key that sets this default is **EMSGenerateSmallMemoryDump**, which is located here:

```
HKLM\SOFTWARE\Cisco Systems,
Inc.\ICM\

```

The value of 0x20000032 for this registry key indicates a router full dump will be generated. To generate a mini-dump rather than a full dump, change the last digit to 1 so that the value is 0x20000031.

The middle six digits of the registry key value determine the number of dumps that are kept. If, for example, these digits are all zeros (0x20000002), CCE by default keeps only the last five generated dumps for any component. For the CCE router, however, only the three latest dumps are kept (0x20000032) by default, since the size of the full dump can be up to 2GB. Keep disk space usage in mind when selecting the number of dumps you want to retain.

If the CCE Router crashes, provide the full dump (the `.mdmp` file generated under the `icm\<instanceid>ra\logfiles` directory), the PDB file (for example, `router.pdb`) from the `icm\bin` directory, and the associated executable (`router.exe`) from the `icm\bin` directory.



Note The registry key value is set to the default value of `0x20000032` on a new install or upgrade, or whenever you run Web Setup.



CHAPTER 7

Performance Counters

- [Import Unified CCE Data Collector Set Template, on page 97](#)
- [Platform Health Monitoring Counters, on page 98](#)
- [Platform Diagnostic Counters – Automatic Collection, on page 101](#)
- [Component-Specific Counters, on page 109](#)

Import Unified CCE Data Collector Set Template

This chapter describes performance counters supported for Microsoft Windows Performance Monitor to monitor Unified CCE components.

In the Performance Monitor, use the template file, **CCE.xml**, to create a Data Collector Set to capture the standard set of performance counters for the Unified CCE components. On any machine where a Unified CCE component is installed, the template file is installed in the `icm\serviceability\perfmon` directory. After you create a Data Collector set, you can schedule or manually start it to capture the Unified CCE performance counters described in this chapter.

The performance counter log files that this Data Collector Set generates are created as CSV files.



Note The template file may contain component-specific counters for Unified CCE components that are not installed on your machine. Counters for these components are included in the log files with blank values.

Follow these steps to import the template file and create the Data Collector set.

Procedure

-
- Step 1** Start the 32-bit Windows Performance Monitor tool by using the shortcut called Performance Monitor. This shortcut is available in the Cisco Unified CCE Tools folder. Alternatively, you can also launch the 32-bit utility by running the command `mmc /32 perfmon.msc`.
 - Step 2** In the panel on the left, expand **Data Collector Sets**.
 - Step 3** Right click **User Defined** and select **New > Data Collector Set**. The Data Collector Set wizard opens.
 - Step 4** Provide a name for the Data Collector Set and select **Create from a template**. Click **Next**.
 - Step 5** Click **Browse**. Go to `icm\serviceability\perfmon` and select the file **CCE.xml**. Click **Next**.

Step 6 Specify the location where you want to collect the performance counter log. Click **Next**.

Step 7 Select **Save and Close** and click **Finish**.

The Performance Monitor creates the Data Collector Set by importing the XML file. You can edit the Data Collector Set to modify the component monitoring, for example to change the sampling interval or add or remove counters. For more information, see "Creating Data Collector Sets" in the Performance Monitor online help.

Platform Health Monitoring Counters

The following table lists the performance counters that you should watch on a regular basis to determine the health of the contact center application.

Threshold values are not monitored by the application itself – alarms are not generated if threshold are exceeded. The responsibility for polling and threshold alarming is extended to the management station.

Table 15: Performance Counters - Health Monitoring

Counter Name (Instance)	Property	Value
% Processor Time (_Total)	Performance Object	Processor
	Type	Int32
	Units (Range)	Percentage (0 - 100%)
	Threshold (Green)	< 50%
	Threshold (Yellow)	50% - 60%
	Threshold (Red)	> 60% (sustained)
	Description	Primary indicator of processor activity; displays the average percentage of CPU busy time observed during the sample interval.
Processor Queue Length	Performance Object	System
	Type	Int32
	Units (Range)	# threads
	Threshold (Green)	< 2 * #CPUs
	Threshold (Yellow)	—
	Threshold (Red)	>= 2 * #CPUs (sustained)
	Description	Number of threads in the processor queue waiting to be serviced. Microsoft states that Processor Queue Length is OK up to 10 per CPU. This may be the case for non-real time applications but Unified CC performance is impacted if this queue length is excessive for a sustained period of time. Timeouts are likely if the server becomes CPU bound or a single application (or process) monopolizes the CPU.

Counter Name (Instance)	Property	Value
Available Bytes	Performance Object	Memory
	Type	Int32
	Units (Range)	Percentage (0 - 100%)
	Threshold (Green)	> 30%
	Threshold (Yellow)	20% - 30%
	Threshold (Red)	< 20%
	Description	Amount of physical memory available to running processes; threshold values are a percentage of physical memory. This is a snap shot—not a running average. Sustained samples below 20% (available) may be indicative of a memory leak.
Pages / sec	Performance Object	Memory
	Type	Int32
	Units (Range)	# page faults
	Threshold (Green)	< 10
	Threshold (Yellow)	>= 10
	Threshold (Red)	> 10 (sustained)
	Description	Pages/sec is the rate at which pages are read from or written to disk to resolve hard page faults. Excessive page faults adversely impacts performance – root cause must be investigated.
Avg. Disk Queue Length (_Total)	Performance Object	Physical Disk
	Type	Float
	Units (Range)	Average # read/write requests
	Threshold (Green)	< 1.5
	Threshold (Yellow)	—
	Threshold (Red)	>= 1.5 (sustained)
	Description	Average number of both read and write requests that were queued for the selected disk during the sample interval.
% Disk Time (_Total)	Performance Object	Physical Disk
	Type	Int32
	Units (Range)	Percentage (0 - 100%)
	Threshold (Green)	< 60%
	Threshold (Yellow)	60% - 80%
	Threshold (Red)	> 80%
	Description	Percentage of elapsed time that the disk drive was busy servicing read or write requests.

Counter Name (Instance)	Property	Value
Bytes Total/sec	Performance Object	Network Interface
	Type	Int32
	Units (Range)	Percentage (0 - 100%)
	Threshold (Green)	< 25%
	Threshold (Yellow)	25% - 30%
	Threshold (Red)	> 30%
	Description	Rate at which bytes are sent and received over each network adapter. Threshold values are a percentage of available bandwidth.
Output Queue Length	Performance Object	Network Interface
	Type	Int32
	Units (Range)	# packets in queue
	Threshold (Green)	0
	Threshold (Yellow)	1
	Threshold (Red)	> 1 (sustained)
	Description	Length of the output packet queue (in packets). If too large, there are delays and the bottleneck should be found and eliminated.
Buffer cache hit ratio	Performance Object	SQLServer:Buffer Manager
	Type	Int32
	Units (Range)	Percentage (0 - 100%)
	Threshold (Green)	> 90%
	Threshold (Yellow)	—
	Threshold (Red)	< 90%
	Description	<p>This counter shows the percentage of pages in the buffer pool without needing to read from disk. Thresholds are expressed as a percentage of hits; instances in which the requested page was found in the cache.</p> <p>This counter is typically a good indicator of whether there is sufficient RAM installed in the server.</p> <p>If you are using SQL Server Standard Edition in a large enterprise or hosted environment and this counter (as well as other performance counters) is not within the correct range, upgrading SQL Server to Enterprise Edition may be the next step. Upgrading SQL Server to Enterprise Edition requires an upgrade of the operating system to Windows Server Enterprise Edition. See Microsoft documentation for details.</p>

Platform Diagnostic Counters – Automatic Collection

The Node Manager samples and collects counter values automatically. The counter values are stored in a disk file on the server and are sampled at one-minute intervals.

Data files contain a rolling window of counter values—older data is discarded in place of new data. Data is stored in multiple files (with a maximum size of 1 MB each) and saved for a maximum of 45 days.

Platform Diagnostic Counter Values

Data file location

\icm\logs

File naming convention

Perf_MACHINENAME_YYYYMMDDHHMMSS.CSV

Where

- *MACHINENAME* is the assigned Windows computer name.
- *YYYYMMDD* is the year, month, day the file was created.
- *HHMMSS* is the hour:minute:second the file was created.

Analysis of these counter values is beneficial when diagnosing a problem with a Unified CCE application component.

Table 16: Performance Counters - Diagnostics

Counter Name	Property	Value
% Processor Time (_Total)	Component	Processor
	Type	Int32
	Units (Range)	Percentage (0 – 100%)
	Description	% Processor Time is the percentage of elapsed time that the processor spends to run a non-Idle thread. It is calculated by measuring the duration that the idle thread is active in the sample interval, and subtracting that time from interval duration. (Each processor has an idle thread that consumes cycles when no other threads are ready to run.) This counter is the primary indicator of processor activity and displays the average percentage of busy time observed during the sample interval. It is calculated by monitoring the time that the service is inactive and subtracting that value from 100%.
Handle Count (_Total)	Component	Process
	Type	Int32
	Units (Range)	# handles
	Description	The total count of handles currently open by this process. This number is equal to the sum of the handles currently open by each thread in this process.

Counter Name	Property	Value
Page Faults / sec	Component	Memory
	Type	Int32
	Units (Range)	# faults
	Description	Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation; hence, this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory). Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.
Committed Bytes	Component	Memory
	Type	Int32
	Units (Range)	# bytes
	Description	Committed Bytes is the amount of committed virtual memory, in bytes. Committed memory is the physical memory that has space reserved on the disk paging files. There can be one or more paging files on each physical drive. This counter displays the last observed value only; it is not an average.
Pages / sec	Component	Memory
	Type	float
	Units (Range)	# pages per second
	Description	Pages/sec is the number of pages either read from the disk or written to the disk to resolve memory references to pages that were not in memory at the time of the reference. Pages/sec is the sum of Pages Input/sec and Pages Output/sec. This counter includes paging traffic on behalf of the system cache to access file data for applications. This is also the primary counter to observe if you are concerned about excessive memory pressure (thrashing) and the excessive paging that may result. This counter, however, also accounts for such activity as the sequential reading of memory mapped files, whether cached or not.
Threads	Component	System
	Type	Int32
	Units (Range)	# threads
	Description	Threads is the number of threads in the computer at the time of data collection. This is an instantaneous count, not an average over the time interval. A thread is the basic executable entity that can run instructions in a processor.

Counter Name	Property	Value
Processor Queue Length	Component	System
	Type	Int32
	Units (Range)	# threads
	Description	Processor Queue Length is the number of threads in the processor queue. Unlike the disk counters, this counter shows ready threads only, not threads that are running. There is a single queue for processor time even on computers with multiple processors. Therefore, if a computer has multiple processors, you must divide this value by the number of processors servicing the workload. A sustained processor queue of fewer than 10 threads per processor is generally acceptable, dependent on the workload.
Processes	Component	System
	Type	Int32
	Units (Range)	# processes
	Description	Processes is the number of processes in the computer at the time of data collection. This is an instantaneous count, not an average over the time interval. Each process represents the running of a program.

Table 17: Performance Counters - Diagnostics

Counter Name	Property	Value
% Processor Time (_Total)	Component	Processor
	Type	Int32
	Units (Range)	Percentage (0 – 100%)
	Description	% Processor Time is the percentage of elapsed time that the processor spends to run a non-Idle thread. It is calculated by measuring the duration that the idle thread is active in the sample interval, and subtracting that time from interval duration. (Each processor has an idle thread that consumes cycles when no other threads are ready to run.) This counter is the primary indicator of processor activity and displays the average percentage of busy time observed during the sample interval. It is calculated by monitoring the time that the service is inactive and subtracting that value from 100%.
Handle Count (_Total)	Component	Process
	Type	Int32
	Units (Range)	# handles
	Description	The total count of handles currently open by this process. This number is equal to the sum of the handles currently open by each thread in this process.

Counter Name	Property	Value
Page Faults / sec	Component	Memory
	Type	Int32
	Units (Range)	# faults
	Description	Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation; hence, this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory). Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.
Committed Bytes	Component	Memory
	Type	Int32
	Units (Range)	# bytes
	Description	Committed Bytes is the amount of committed virtual memory, in bytes. Committed memory is the physical memory that has space reserved on the disk paging files. There can be one or more paging files on each physical drive. This counter displays the last observed value only; it is not an average.
Pages / sec	Component	Memory
	Type	float
	Units (Range)	# pages per second
	Description	Pages/sec is the number of pages either read from the disk or written to the disk to resolve memory references to pages that were not in memory at the time of the reference. Pages/sec is the sum of Pages Input/sec and Pages Output/sec. This counter includes paging traffic on behalf of the system cache to access file data for applications. This is also the primary counter to observe if you are concerned about excessive memory pressure (thrashing) and the excessive paging that may result. This counter, however, also accounts for such activity as the sequential reading of memory mapped files, whether cached or not.
Threads	Component	System
	Type	Int32
	Units (Range)	# threads
	Description	Threads is the number of threads in the computer at the time of data collection. This is an instantaneous count, not an average over the time interval. A thread is the basic executable entity that can run instructions in a processor.

Counter Name	Property	Value
Processor Queue Length	Component	System
	Type	Int32
	Units (Range)	# threads
	Description	Processor Queue Length is the number of threads in the processor queue. Unlike the disk counters, this counter shows ready threads only, not threads that are running. There is a single queue for processor time even on computers with multiple processors. Therefore, if a computer has multiple processors, you must divide this value by the number of processors servicing the workload. A sustained processor queue of fewer than 10 threads per processor is generally acceptable, dependent on the workload.
Processes	Component	System
	Type	Int32
	Units (Range)	# processes
	Description	Processes is the number of processes in the computer at the time of data collection. This is an instantaneous count, not an average over the time interval. Each process represents the running of a program.
% Idle Time (0 C:)	Component	Physical Disk
	Type	Float
	Units (Range)	Percentage (0 - 100%)
	Description	% Idle Time reports the percentage of time during the sample interval that the disk was idle. Note This instance is for the virtual machine's drive C—the drive where the software is installed and where logs are stored.
% Idle Time (1 E:)	Component	Physical Disk
	Type	Float
	Units (Range)	Percentage (0 - 100%)
	Description	% Idle Time reports the percentage of time during the sample interval that the disk was idle. Note This instance is for the virtual machine's drive E—the drive where the database is stored. If the component on this virtual machine does not have a database component, the counter sample values appear as <code>ERROR</code> , but this has no adverse effect on the component itself.

Counter Name	Property	Value
Avg. Disk Queue Length (0 C:)	Component	Physical Disk
	Type	Float
	Units	# requests
	Description	<p>Avg. Disk Queue Length is the average number of both read and write requests that were queued for the selected disk during the sample interval.</p> <p>Note This instance is for the virtual machine's drive C—the drive where the software is installed and where logs are stored.</p>
Avg. Disk Queue Length (1 E:)	Component	Physical Disk
	Type	Float
	Units (Range)	# requests
	Description	<p>Avg. Disk Queue Length is the average number of both read and write requests that were queued for the selected disk during the sample interval.</p> <p>Note This instance is for the virtual machine's drive E—the drive where the database is stored. If the component on this virtual machine does not have a database component, the counter sample values appear as <code>ERROR</code>, but this has no adverse effect on the component itself.</p>
Avg. Disk sec/Read (0 C:)	Component	Physical Disk
	Type	Float
	Units	seconds
	Description	<p>Avg. Disk sec/Read is the average time, in seconds, of a read of data from the disk.</p> <p>Note This instance is for the virtual machine's drive C—the drive where the software is installed and where logs are stored.</p>
Avg. Disk sec/Read (1 E:)	Component	Physical Disk
	Type	Float
	Units	seconds
	Description	<p>Avg. Disk sec/Read is the average time, in seconds, of a read of data from the disk.</p> <p>Note This instance is for the virtual machine's drive E—the drive where the database is stored. If the component on this virtual machine does not have a database component, the counter sample values appear as <code>ERROR</code>, but this has no adverse effect on the component itself.</p>

Counter Name	Property	Value
Avg. Disk sec/Write (0 C:)	Component	Physical Disk
	Type	Float
	Units	seconds
	Description	Avg. Disk sec/Write is the average time, in seconds, of a write of data to the disk. Note This instance is for the virtual machine's drive C—the drive where the software is installed and where logs are stored.
Avg. Disk sec/Write (1 E:)	Component	Physical Disk
	Type	Float
	Units	seconds
	Description	Avg. Disk sec/Write is the average time, in seconds, of a write of data to the disk. Note This instance is for the virtual machine's drive E—the drive where the database is stored. If the component on this virtual machine does not have a database component, the counter sample values appear as <code>ERROR</code> , but this has no adverse effect on the component itself.

Platform Diagnostic Counters

All Components

If a problem occurs on a Unified CCE/Unified ICM component, to further diagnose the problem, enable these counters using the Windows PerfMon tool (On Windows server, Start > Cisco Unified CCE Tools > Performance Monitor). At first, set the interval to 15 seconds and collect a sample large enough before, during, and after the problem. Save the data in .CSV format for simple import into Microsoft Office Excel. Attach the file to the TAC case.

If the data does not provide enough resolution to diagnose root cause, increase the interval to 5 seconds. A sample interval more frequent than 3 seconds should not be attempted.

Table 18: Diagnostic Counters - All Components

Performance Object	Instance	Counter Name
LogicalDisk	_Total	Avg. Disk Queue Length
LogicalDisk	C:	Avg. Disk Queue Length
LogicalDisk	<>	Avg. Disk Queue Length
Network Interface	<NIC Name>	Packets Outbound Discarded
PhysicalDisk	_Total	Disk Transfers/sec
Process	_Total	Page Faults/sec

Performance Object	Instance	Counter Name
Process	_Total	Virtual Bytes
Process	_Total	Working Set
Processor	_Total	Interrupts/sec
Process	<virus scanner>	% Processor Time
Process	<virus scanner>	Page Faults/sec
Process	<virus scanner>	Virtual Bytes
Process	<virus scanner>	Working Set

Logger/Administration & Data Server/HDS

These counters are intended for Unified CCE/Unified ICM components that have a SQL Server database installed. SQL Server counters are listed in the next session.

Set the initial sample frequency to 15 seconds. If the resolution is insufficient, decrease the frequency to 5 seconds.

Table 19: Diagnostic Counters - Logger, Administration & Data Server, and HDS

Performance Object	Instance	Counter Name
Physical Disk	<>	% Disk Time
Physical Disk	<>	Avg. Disk Queue Length
Physical Disk	<>	Disk Transfers/sec
Process	** See note	% Processor Time
Process	** See note	Page Faults/sec
Process	** See note	Virtual Bytes
Process	** See note	Working Set
Process	sqlservr	% Processor Time
Process	sqlservr	Page Faults/sec
Process	sqlservr	Virtual Bytes
Process	sqlservr	Working Set



Note Logger Processes: configlogger, histlogger, recovery, replication
AW/HDS Processes: configlogger, replication, rtclient, rtdist

SQL Server

The listed counters are available on those servers on which a Unified CCE/Unified ICM database is installed. Set the initial sample frequency to 15 seconds. If the resolution is insufficient, decrease the frequency to 5 seconds.

Table 20: Diagnostic Counters - SQL Server

Performance Object	Instance	Counter Name
SQLServer:Access Methods		Full Scans/sec
SQLServer:Buffer Manager		Buffer cache hit ratio
SQLServer:Buffer Manager		Page reads/sec
SQLServer:Buffer Manager		Page writes/sec
SQLServer:Buffer Manager		Stolen pages
SQLServer:Databases	_Total	Transactions/sec
SQLServer:Databases	cscs_awdb ¹	Transactions/sec
SQLServer:Databases	cscs_hds ²	Transactions/sec
SQLServer:General Statistics		User Connections
SQLServer:Latches		Average Latch Wait Time (ms)
SQLServer:Locks	_Total	Lock Timeouts/sec
SQLServer:Locks	_Total	Number of Deadlocks/sec
SQLServer:Memory Manager		Memory Grants Pending

¹ Where “cscs” is the Unified ICM/Unified CCE instance name.

² Where “cscs” is the Unified ICM/Unified CCE instance name.

Component-Specific Counters

Performance counters that measure time durations in milliseconds, provide granular measurements of at least 16 milliseconds.



Note To enable a counter that is disabled by default, make a change to the registry.

Performance counter-objects that are being captured or monitored as "per second" or rate values, are interpreted as average number of operations completed during each second of the sample interval. This is a computed value, and the performance monitor tool essentially uses the following formula to represent the counter value.

All such **perfmon counters** that represent rate values are defined as either "PERF_COUNTER_COUNTER" or "PERF_COUNTER_BULK_COUNT" type.

PERF_COUNTER_COUNTER / PERF_COUNTER_BULK_COUNT Calculations:

Table 21: Calculating PERF_COUNTER_COUNTER or PERF_COUNTER_BULK_COUNT

$\text{PERF_COUNTER_COUNTER} = (N1 - N0) / ((D1 - D0) / F)$	
Numerator (N)	The numerator (N) represents the number of operations performed during the last sample interval
Denominator (D)	The denominator (D) represents the number of ticks elapsed during the last sample interval
F	F is the frequency of the ticks.



Note For example, if the VRU PIM **perfmon counter** for "New Calls/sec" is set up to capture the counter value in every 5 seconds, and during that interval the VRU PIM receives 15 calls, then the rate value shown is 3 calls / sec.

Router

Performance Object
Cisco ICM Router

Counter Instance

“{ICM Instance Name}” – if multiple instances installed

Table 22: Router Performance Counters

Always ON?	Counter Name	Description
Y	Agents Logged On These counters are also quite useful for long-term trending to determine whether there are capacity issues now or whether there are in the future. The counter values can be compared to other PerfMon counters (for example, CPU, Memory, Disk, and NIC). Relationships and cause/effect analysis can greatly assist in confirming existing or predicting upcoming capacity/performance problems.	The number of (contact center) agents currently logged in.
Y	Calls In Progress	The number of calls currently in progress (being controlled by the CCE application).
Y	Active Agent Answers Enabled Calls	Total number of active calls on which Agent Answers is enabled, for a CCE instance. The Agent Answers service silently monitors a call and displays relevant real-time suggestions to agents and supervisors in Finesse gadgets. These suggestions enrich an agent's ability to respond to a caller.
Y	Calls/sec	The (calculated) inbound call rate measured in the number of calls received per second.
Y	Calls In Queue	The number of calls queued in all network Voice Response Units (VRUs), from the router's perspective, including those calls that are in the process of transferring to the VRU for queuing.
Y	Calls In Router	The number of active calls in the router, including the calls sent to VRU for treatment or queuing and the calls the router is waiting for response from the routing client.
Y	CSNRequestsPerSec	The number of contact share node requests received per second.
Y	CSNRequestsAvgRespTime	Average time taken to respond to contact share node requests. Time is mentioned in milliseconds (ms).
Y	CSNNumberSGUpdates	Total Number of Skill Group updates from the target CCE systems at every Live Data-published interval (default 3 sec).
Y	CSNNumberPQUpdates	Total Number of PQ updates from the target CCE systems at every Live Data-published interval (default 3 sec).
Y	Pending PQ Count	Total number of precision queue configuration operations in the system yet to be fully processed.
Y	Pending PQ Agent Count	Total number of agents yet to be evaluated or handled following one or more precision queue configuration operations.

Always ON?	Counter Name	Description
Y	Average PQ Update Time	Average time to completely process a precision queue configuration update. Average time is calculated as the moving average for the last 10 precision queue configuration updates.
N	Size	The current Router state size - the total size of all of the state transfer objects in Router memory; this size is measured in kilobytes. After one Router side goes out of service, when it returns in-service, the Router state is transferred from the surviving Router side to the returning Router side.
N	Messages Processed/sec	The number of MDS messages that the Router processed. By default, this counter is disabled.
N	Bytes Processed/sec	The rate at which the Router processed the data bytes. By default, this counter is disabled.
N	Avg Process Time/Message (ms)	The average time (in milliseconds) that the Router spends processing an MDS message.
N	Max Process Time(ms)	The maximum time (in milliseconds) that the Router spends processing an MDS message.

Enable Optional Counters

Key

HKEY_LOCAL_MACHINE_SOFTWARE\Cisco Systems,
Inc.\ICM*<Instance>**<node>*\Router\CurrentVersion\Debug

Name

PerfmonCounterInterval

Type

REG_DWORD

Default

0

Enabled

1

Logger

Performance Object

Cisco ICM Logger

Counter Instance

"{ICM Instance Name}" – if multiple instances installed

Table 23: Logger Performance Counters

Always ON?	Counter Name	Description
Y	Number of DB Write Records	The number of database writes (records/rows) in the historical logger process that is written to the database at the time the counter is polled.

Always ON?	Counter Name	Description
Y	DB Write Average Time	The average database write time expresses the average amount of time, in 100 nanosecond units, required to write data to a table in the central controller database. This value represents the average time per write of the write operations that occurred in the past second. This object is a good indicator of contention for database access.
Y	DB Write Records Processed	The number of records processed – written to the database – in the Historical Logger Process in the past second.

Administration & Data Server

Performance Object

Cisco ICM Distributor RealTime

Counter Instance

{Instance Name} ADS#

Table 24: Administration & Data Server Real-Time Counter

Always ON?	Counter Name	Description
Y	Agent Queue Depth	The queue depth – number of pending write transactions – for the Agent table in the Real-time Client process.
Y	Agent DB Write Average Time	The average time – in units of 100 ns – for the Real-time Client process to write an Agent table transaction within the past 1 second interval.
Y	Agent DB Write Records Processed	The number of Agent table records written by the Real-time Client process in the past 1 second interval.
Y	Agent Skill Group Queue Depth	The queue depth – number of pending write transactions – for the Agent Skill Group table in the Real-time Client process.
Y	Agent Skill Group DB Write Average Time	The average time – in units of 100 ns – for the Real-time Client process to write an Agent Skill Group table transaction within the past 1 second interval.
Y	Agent Skill Group DB Write Records Processed	The number of Agent Skill Group table records written by the Real-time Client process in the past 1 second interval.
Y	Skill Group Queue Depth	The queue depth – number of pending write transactions – for the Skill Group table in the Real-time Client process.
Y	Skill Group DB Write Average Time	The average time – in units of 100 ns – for the Real-time Client process to write an Skill Group table transaction within the past 1 second interval.
Y	Skill Group DB Write Records Processed	The number of Skill Group table records written by the Real-time Client process in the past 1 second interval.
Y	CallType Queue Depth	The queue depth – number of pending write transactions – for the CallType table in the Real-time Client process.
Y	CallType DB Write Average Time	The average time – in units of 100 ns – for the Real-time Client process to write an CallType table transaction within the past 1 second interval.

Always ON?	Counter Name	Description
Y	CallType DB Write Records Processed	The number of CallType table records written by the Real-time Client process in the past 1 second interval.
Y	Route Queue Depth	The queue depth – number of pending write transactions – for the Route table in the Real-time Client process.
Y	Route DB Write Average Time	The average time – in units of 100 ns – for the Real-time Client process to write an Route table transaction within the past 1 second interval.
Y	Route DB Write Records Processed	The number of Route table records written by the Real-time Client process in the past 1 second interval.
Y	Service Queue Depth	The queue depth – number of pending write transactions – for the Service table in the Real-time Client process.
Y	Service DB Write Average Time	The average time – in units of 100 ns – for the Real-time Client process to write an Service table transaction within the past 1 second interval.
Y	Service DB Write Records Processed	The number of Service table records written by the Real-time Client process in the past 1 second interval.

Performance Object

Cisco ICM Distributor Replication

Counter Instance

{Instance Name} Distributor #

Table 25: Administration & Data Server Replication Counters

Always ON?	Counter Name	Description
Y	DB Write Average Time	The average time – in units of 100 nanoseconds – for database write operations in the HDS Replication process during the past 1 second interval.
Y	DB Write Records Processed	The number of records written by the HDS Replication process in the past 1 second interval.

PG – OPC**Performance Object: Default**

Cisco ICM OPC

Optionally Enabled

Cisco ICM OPC (Optional)

Counter Instance

“{Instance Name} PG#A/B” (For example, “acme PG3A”)

Table 26: PG - OPC Counters

Always ON?	Counter Name	Description
Y	Call Count	Number of calls that are currently active.
N	Agent Count	Number of agents that are configured in the system. An agent is a specific individual who receives calls through the peripheral.

Always ON?	Counter Name	Description
Y	Active Agent Answers Enabled Calls	Total number of active calls on which Agent Answers is enabled, for a given peripheral gateway. The Agent Answers service silently monitors a call and displays relevant real-time suggestions to agents and supervisors in Finesse gadgets. These suggestions enrich an agent's ability to respond to a caller.
N	Skill Group Count	This counter provides the number of various skill groups available for the agents to sign in. A skill group is a group of agents who share a common set of skills and who can, therefore, all handle specific types of calls. Each skill group contains one or more agents. If supported by the peripheral, each agent can be a member of more than one skill group.
N	Services Count	This counter provides the number of services that are configured to process the calls. A service is a type of processing that the caller requires. A peripheral might have services defined for sales, technical support, or opening new accounts. Each service has one or more skill groups whose members can provide the service. Each skill group can be associated with more than one service.
Y	Logged-In Agent Count	Number of agents that have logged in. This does not necessarily indicate that the agents are ready to accept calls.
Y	Ready Agent Count	Number of Agents that are logged in and are ready to accept calls.
N	Not-Ready Agent Count	Number of Agents that are logged in, but occupied with tasks other than accepting incoming calls.
Y	Talking Agent Count	Number of Agents currently talking on Inbound or Outbound calls.
N	Held Agent Count	Number of Agents that are inactively participating in a call.
N	Work-Ready Agent Count	Agents occupied with work associated with the last call. This implies that the agent is no longer connected to the call and is ready to receive additional calls when they exit this state.
N	Work-Not-Ready Agent Count	Agents occupied with work associated with the last call. This implies that the agent is no longer connected to the call. These Agents are not ready to receive additional calls when they exit this state.
N	Logged-Out Agent Count	Number of Agents that are logged out of the system. This count helps in validating the statistics if there are any state mismatches.
N	None-State Call Count	This counter provides the number of calls for which a call object was created but no activity.
N	Null-State Call Count	This counter provides the number of calls that has no relationship between the call and the device.
N	Initiated Call Count	This counter provides the number of calls for which the device has requested for a service. Often this is the dialing state.

Always ON?	Counter Name	Description
N	Alerting Call Count	This counter provides the number of calls for which the device is in alerting (ringing) state. This indicates that a call wishes to become connected to a device.
Y	Connected Call Count	This counter provides the number of calls for which the device is actively participating in the call.
N	Held Call Count	This counter provides the number of calls for which the device is inactively participating in the call.
N	Queued Call Count	This counter provides the number of calls for which the general state progression has been stalled. This state generally refers to two conditions but can apply to others as well. One condition is when a device is trying to establish a connection with a call, and the process is stalled. The second condition is when a call tries to establish a connection with a device and that process is stalled.
N	Failed Call Count	This counter provides the number of calls for which the general state progression has been closed. This state generally refers to the condition when a device tries to become connected to a call or a call tries to become connected to a device and the attempt fails. Failed can result because of failure to connect the calling device and call, failure to connect the called device and call, failure to create the call, and other reasons.

Enable optional counters

Key

```
HKEY_LOCAL_MACHINE_SOFTWARE\Cisco Systems,  
Inc.\ICM\

```

Name

```
OPCOptionalPerfmonCounters
```

Type

```
REG_DWORD
```

Default

```
0
```

Enabled

```
1
```

PG – Communications Manager (EA) PIM

Performance Object: Default

```
Cisco ICM CMPIM
```

Optionally Enabled

```
Cisco ICM CMPIM (Optional)
```

Counter Instance

“{Instance Name} PG#A/B PIM#” (For example, “acme PG3A PIM1”)

Table 27: PG - CM PIM Counters

Always ON?	Counter Name	Description
N	Agent Count	Number of agents that are currently configured in system.
N	Calls per sec	Number of incoming calls per second.
Y	Call Count	Number of calls that are in progress.
N	Invalid Call Count	Number of calls that are not in any of the valid call states.
N	Messages per second	Number of call events, agent events exchanged per second between the JTAPI Gateway and CM PIM.
N	Messages sent	Number of call events, agent events, and CSTA messages sent today.
N	Messages sent past 5	Number of call events, agent events, and CSTA messages sent past 5 seconds.

Enable Optional Counters**Key**

HKEY_LOCAL_MACHINE_SOFTWARE\Cisco Systems,
Inc.\ICM*<Instance>*\<PG##>\PG\CurrentVersion\PIMS\pim#\EAGENTData\Dynamic

Name

EnableOptionalCounters

Type

REG_DWORD

Default

0

Enabled

1

PG – VRU PIM**Performance Object**

Cisco ICM VRUPIM

Counter Instance

“{Instance Name} PG#A/B PIM#” (For example, “acme PG3A PIM3”)

Table 28: PG - VRU PIM Counters

Always ON?	Counter Name	Description
Y	Calls At VRU	Calls at VRU is the number of calls that are currently at the Voice Response Unit (VRU). For a VRU that only uses a Call Routing Interface, this value is zero.
N	Messages To VRU/sec	Messages To VRU/sec is the rate at which messages are sent to the Voice Response Unit (VRU). This counter is active only when enabled in ICM registry.
N	Messages From VRU/sec	Messages From VRU/sec is the rate at which messages are received from the Voice Response Unit (VRU). This counter is active only when enabled in ICM registry.

Always ON?	Counter Name	Description
N	Bytes To VRU/sec	Bytes To VRU/sec is the rate at which bytes are sent to the Voice Response Unit (VRU). This counter is active only when enabled in ICM registry.
N	Bytes From VRU/sec	Bytes From VRU/sec is the rate at which bytes are received from the Voice Response Unit (VRU). This counter is active only when enabled in ICM registry.
Y	New Calls/sec	New Calls/sec is the rate at which new calls arriving at the Voice Response Unit (VRU). New calls are calls not under ICM script control when arriving at a Service Control VRU. The Pre-Routed calls/Sec can be for an entire day. The calls/sec can also be from the time the PIM restarts or for an hour.
Y	Pre-Routed Calls/Sec	Pre-Routed Calls/sec is the rate at which Pre-Routed calls are arriving at Voice Response Unit (VRU). Pre-Routed calls are calls under ICM script control when arriving at a Service Control VRU. The Pre-Routed calls/Sec can be for an entire day. The calls/sec can also be from the time the PIM restarts or for an hour.
Y	Connection Resets	Connection Resets is the number of times the TCP connection between ICM and the Voice Response Unit changed from an established state to a closed state since the application started.

Enable Optional Counters

Key

HKEY_LOCAL_MACHINE_SOFTWARE\Cisco Systems,
Inc.\ICM*<Instance>*\<PG##>\PG\CurrentVersion\PIMS\pim#\VRUData\Dynamic

Name

EnableOptionalPerfmonCounter

Type

REG_DWORD

Default

0

Enabled

1

CTI Server

Performance Object: Default

Cisco ICM CTISVR

Optionally Enabled

Cisco ICM CTISVR (Optional)

Counter Instance

“{Instance Name} CG#A/B” (For example, “acme CG3A”)

Table 29: CTI Server Counters

Always ON?	Counter Name	Description
N	Reported Call Count	Number of calls that are already reported to the CTI clients.
N	Active Call Count	Number of calls that are currently in progress.
N	Deactivated Call Count	Number of calls that are not currently active and eventually cleared.
N	Cleared Call Count	Number of calls that no longer exist in the system.
N	Private Call Count	Number of calls that are privately tracked by CTI Server and which are not reported to OPC.
Y	Logged-In Agent Count	Agents that have logged in. This does not necessarily indicate that they are ready to accept calls.
Y	Ready Agent Count	Number of Agents that are logged in and are ready to accept calls.
N	Not-Ready Agent Count	Number of Agents that are logged in, but occupied with tasks other than accepting incoming calls.
Y	Talking Agent Count	Number of Agents currently talking on Inbound or Outbound calls.
N	Held Agent Count	Number of Agents that are inactively participating in a call.
N	Work-Ready Agent Count	Agents occupied with work associated with the last call. This implies that agent is no longer connected to the call and is ready to receive additional calls when they exit this state.
N	Work-Not-Ready Agent Count	Agents occupied with work associated with the last call. This implies that agent is no longer connected to the call. These agents are not ready to receive additional calls when they exit this state.
N	Logged-Out Agent Count	The number of Agents that are logged out of the system. This count helps in validating the statistics if there are any state mismatches.
Y	Sessions Unknown	The number of sessions for which there is no socket connection made yet.
N	Sessions Opening	The number of sessions that are in the process of setting up a connection.
Y	Sessions Open	The number of sessions that were successfully setup.
N	Sessions Closing	The number of sessions that are in the process of tear down.
Y	Sessions Closed	The total number of sessions that are terminated by the CTI Server.
Y	Sessions Failed	The number of sessions that failed due to various reasons like missing heartbeat, open request timeout, session inactivity, and so on. These timers are configurable parameters in CTI Server.
Y	Total Sessions	The total number of sessions maintained by CTI Server.

Enable Optional Counters**Key**

HKEY_LOCAL_MACHINE_SOFTWARE\Cisco Systems,
Inc.\ICM*<Instance>*\<CG##>\CG\CurrentVersion\CTIServer\Dynamic

Name

CTISVROptionalCounters

Type

REG_DWORD

Default

0

Enabled

1

CTI OS Server

Performance Object

Cisco ICM CTI OS

Counter Instance

CTI OS Name

Table 30: CTI OS Server Counters

Always ON?	Counter Name	Description
Y	CTI OS Active Client Connections	The number of CTI OS Active Client Mode Desktop Connections. This value indicates the total number of desktops connected to the CTI OS server. The number of desktops connected to the A and B side of CTI OS determine the total desktops connected through this instance of CTI OS server.
Y	CTI OS Active Monitor Mode Connections	The number of CTI OS Active Monitor Mode Desktop Connections. CTI OS only supports two monitor mode connections per each CTI OS server. This value indicates how many monitor mode connections are in use. After there are two in use further monitor mode connection attempts are rejected.
Y	CTI OS Active Calls	The total number of active calls being tracked by CTI OS. This value shows how many calls are currently being handled by CTI OS. This value should go up and down based on the call arrival rate and the agent call completion rate.
Y	CTI OS Configured Skill Groups	The total number of configured skill groups being tracked by CTI OS. This value should match the number of skill groups configured for the PG that this CTI OS is associated.
Y	CTI OS Configured Teams	The total number of configured Teams being tracked by CTI OS. This value should match the number of teams configured for the PG that this CTI OS is associated.
Y	CTI OS Configured Agents	The total number of configured Agents being tracked by CTI OS. This value should match the number of Agents configured for the PG that this CTI OS is associated.
Y	CTI OS Active Conferences	The total number of active Conferences being tracked by CTI OS. This value indicates the number of multi-party calls that are in progress at any one given time in CTI OS.

Always ON?	Counter Name	Description
Y	CTI OS Call Count	The total number of calls handled by CTI OS. This value only increases and shows the total number of calls processed by CTI OS since it last started. This value should increase at the same rate as the calls per second being shown by the Router.
Y	CTI OS Conference Count	The total number of Conferences performed by CTI OS. This value only increases and shows the total number of calls that were conferenced since CTI OS last started. The conference count should be a small percentage of total calls.
Y	CTI OS Transfer Count	The total number of Transfers performed by CTI OS. This value only increases and shows the total number of calls that were transferred since CTI OS last started. The transfer count should be a small percentage of total calls.
Y	CTI OS Call Failed Count	The total number of Calls that failed reported to CTI OS. This value shows the total number of calls that failed via a failure event being reported to CTI OS. If this count begins to rise the log file should be captured to gather more specific information about the failure events.
Y	CTI OS CTI Message Receive Rate (msg/sec)	The rate at which CTI OS receives messages from CTI Server per second. This value is an indicator to total load on the system. Increases are not really a problem unless the CTI OS Service Broker Queue Size also begins to increase.
Y	CTI OS CTI Message Send Rate (msg/sec)	The rate at which CTI OS sends messages to CTI Server per second. This value is an indicator of total load on the system. If it increases it indicate the CTI OS server is under a heavy request load from the desktop clients.
Y	CTI OS Service Broker Queue Size	The number of messages queued in the CTI OS Service Broker queue. This value is a good load indicator for CTI OS. If it increases, it can indicate that CTI OS is not keeping up with the incoming message rate from CTI Server. A review of the configuration may be necessary to understand why CTI OS is not able to keep up with event handling from CTI Server.
N	CTI OS Call Object Count	The total number of CTI OS call objects that are active. This value shows how many CTI OS Call objects were created since it last started. This value should go up and down and may reach a steady state when the number of calls being completed by agents equals the call arrival rate.
N	CTI OS Connection Object Count	The total number of active CTI OS connection objects. This value shows how many CTI OS connection objects were created since it last started. This value should go up and down and may reach a steady state when the number of calls being completed by agents equals the call arrival rate.
N	CTI OS Argument Object Count	The total number of active CTI OS argument objects. This value shows how many CTI OS argument objects were created since it last started. This value shall be quite large, go up and down and may reach a steady state when the number of calls being completed by agents equals the call arrival rate.
N	CTI OS Device Object Count	The total number of active CTI OS devices. This value shows how many CTI OS device objects were created since it last started. This value should mainly stay constant while CTI OS runs.
N	CTI OS Agent Object Count	The total number of CTI OS agent objects. This value shows how many CTI OS agent objects were created since it last started. This value should stay constant while CTI OS runs unless agents are added or deleted.

Always ON?	Counter Name	Description
N	CTI OS Skill group Object Count	The total number of CTI OS skill group objects. This value shows how many CTI OS skill group objects were created since it last started. This value should stay constant while CTI OS runs unless skill groups are added or deleted.
N	CTI OS Supervisor Object Count	The total number of CTI OS Supervisor objects. This value shows how many CTI OS supervisor objects were created since it last started. This value should stay constant while CTI OS runs unless supervisors are added or deleted.
N	CTI OS Team Object Count	The total number of CTI OS Team objects. This value shows how many CTI OS team objects were created since it last started. This value stays constant while CTI OS runs unless teams are added or deleted.
N	CTI OS Total Objects Created Count	The total count of all objects created by CTI OS. This value shows how many CTI OS objects were created since it last started. This value only increases and grows very large as CTI OS up time increases.
N	CTI OS Total Objects Deletion Count	The total count of all objects deleted by CTI OS. This value shows how many CTI OS objects were deleted since it last started. This value only increases and grows very large as CTI OS up time increases. It never equals the total objects created count as some objects are never deleted after being created by CTI OS like agent, device, team and skill group objects.
N	CTI OS Active Object Count	The total count of all objects created by CTI OS that are active. This value shows how many CTI OS objects are currently allocated since it last started. If this value begins to increase it would indicate that a memory leak is occurring in CTI OS. The specific object counters show which object is not being released.
Y	CTI OS CLIENT Send Message Rate (msg/sec)	The rate at which CTI OS sends messages to Clients per second. This value shows the number of messages, per second, that CTI OS is delivering messages to CTI OS desktops. As this value increases it indicates that CTI OS server is being placed under an increasing load. A review of the configuration as it relates to agents, skill groups and teams may be necessary.
Y	CTI OS CLIENT Receive Message Rate (msg/sec)	The rate at which CTI OS receives messages from Clients per second. This value shows the number of messages, per second, that are being received from the CTI OS desktops. As this value increases it indicates that CTI OS is being placed under an increasing request load from the desktops.
Y	CTI OS CLIENT Total Number of Pending Write Operations	The total number of pending write operations for all clients. This value shows the total number of messages in the system waiting to be read by CTI OS clients. If the value increases, it can indicate that there are one or more clients not keeping up with reading messages from CTI OS.
Y	CTI OS CLIENT Total Message Buffer Size (Bytes)	The total number of bytes used to store the pending writes for all clients. This value shows the total amount of memory used to store all the messages that are waiting to be read by CTI OS clients.
Y	CTI OS CG Receive Queue Size	The number of messages queued in the CTI OS CG Receive Queue. This value is an indicator of the total load on the system. If it increases, a review of the configuration may be necessary to understand why CTI OS is not keeping up with the incoming message rate from the CTI Server.

Enable Optional Counters**Key**

HKEY_LOCAL_MACHINE_SOFTWARE\Cisco Systems,
Inc.\ICM\{instance}\CTIOS#\EMS\CurrentVersion\Library\Processes\ctios

Name

EMSTraceMask

Type

REG_DWORD

Enable

0x200000

Outbound Option Campaign Manager

Performance Object

Cisco ICM CampaignMgr

Counter Instance

"{Instance Name}"

Table 31: Outbound Option Campaign Manager Counters

Always ON?	Counter Name	Description
Y	DB Space Utilization	The Campaign Manager and Import processes share a private database on the Logger. This counter reports the percentage of allocated space in the database that is currently utilized. An administrator should consider increasing the database size when the value of this counter exceeds eighty percent (80%).
Y	Queue Depth	The Campaign Manager is a multithreaded process. There is one main dispatch thread that is involved in most processing. Queue Depth indicates how many messages are queued to this internal dispatch thread.
Y	Average Queue Time	The Campaign Manager is a multithreaded process. There is one main dispatch thread that is involved in most processing. This counter reports the average time spent in the main dispatch thread queue in milliseconds.
Y	Do Not Call Number Count	The Campaign Manager manages a global list of phone numbers used to prevent block dialing. This list is stored in memory. Each record uses 17 bytes of memory. This counter shows how many do not call entries are currently in memory.
Y	Active Dialer Count	The Campaign Manager process feeds one or more Dialer components; each Dialer dials customer numbers for outbound campaigns. This counter indicates how many Dialers are currently registered to the Campaign Manager.

Always ON?	Counter Name	Description
Y	Congestion Level	This counter returns the current Campaign Manager congestion level. The Campaign Manager becomes congested when it cannot process the volume of inbound messages from dialers quickly enough. Congestion control engages when the Campaign Manager message queue depth reaches predefined thresholds. As each level is reached, the Campaign Manager instructs dialers to slow the dialing rate to a sustainable level. When congestion eases to a lower level, the Campaign Manager signals for an increased dialing rate. The congestion levels are: <ul style="list-style-type: none"> • 0 - Normal operation • 1 - Slightly congested • 2 - Moderately congested • 3 - Heavily congested
Y	Replication Pending Files	This counter returns the number of pending files that await replication from this side.
Y	Replication Pending Kilo Bytes	This counter returns the amount of data (in KB) that await replication from this side.

Outbound Option Import

Performance Object

Cisco ICM Import

Counter Instance

“{Instance Name}”

Table 32: Outbound Option Import Counters

Always ON?	Counter Name	Description
Y	Records Imported Today	The Outbound Option Import process imports customer records that contain phone numbers used by the Campaign Manager and Dialer to find available customers for a campaign. This counter tracks how many records were imported today.

Outbound Option Dialer

Performance Object

Cisco ICM Dialer

Counter Instance

“{Instance Name}”

Table 33: Outbound Option Dialer Counters

Always ON?	Counter Name	Description
Y	Queue Depth	The Dialer is a multithreaded process that communicates between threads using inter thread messaging. This indicates how many messages are currently queued up for the main dispatch thread. By default, the Dialer process restarts when this value exceeds 10,000 messages.
Y	Average Queue Time	The Dialer is a multithreaded process that communicates between threads using messaging. There is one main dispatch thread that is involved in most processing. This shows what is the average time spent in queue.
Y	Talking Agents	For an agent campaign, the Dialer replaces calls to customers and transfers those customers to agents. This counter indicates how many agents are currently talking in the monitored campaign skill group.
Y	Busy Port (Customer) Count	The port is the unit on the Dialer that places calls to reserve agents and to contact customers. This counter tracks how many ports are currently busy trying to contact customers. This includes ports that are actively dialing and those that have been allocated but are not yet dialing a customer.
Y	Ports Actively Dialing Customer Count	The port is the unit on the Dialer that places calls to reserve agents and to contact customers. This counter tracks ports that are currently actively dialing customers.
Y	Busy Port (Reservation) Count	The port is the unit on the Dialer that places calls to reserve agents and to contact customers. This counter tracks how many ports are currently busy reserving agents only for normal records.
Y	Agent Reservation Port Count	The port is the unit on the Dialer that places calls to reserve agents and to contact customers. This counter tracks how many ports are currently being used for reserving agents for both normal and callback records.
Y	Port Utilization Percent	The port is the unit on the Dialer that places calls to reserve agents and to contact customers. This counter tracks the percent of total dialer ports in use for all outbound calls.
Y	Idle Port Count	The port is the unit on the Dialer that places calls to reserve agents and to contact customers. This counter tracks how many ports are currently idle.
Y	PCB Records Cached	The Dialer caches the PCB records received from campaign manager. This counter tracks the total number of PCB records cached.
Y	Idle PCB Records Cached	This counter tracks the number of the cached PCB records that are in the idle state, waiting to be dialed out from the dialer.
Y	Idle Not-Ready PCB Records Cached	This counter tracks the number of cached PCB records in the idle state where Agent is in Not-Ready state. These records will be retried until the agent is ready or the PCB call time expires.
Y	Call Attempt Count	The Dialer attempts to contact customers and transfer them to reserved agents or an available IVR. This counter tracks how many customer attempts were placed today. It does not include preview calls that were rejected or skipped.

Always ON?	Counter Name	Description
Y	Abandoned Call Count	When a customer is contacted and an agent is not available to take the call, the call can be dropped or sent to the IVR for prompting and queuing. When either of these conditions occurs, the call is counted as abandoned. In a transfer to IVR campaign, a call is dropped and counted as abandoned if the configured IVR port limit is exceeded.
Y	Reservation Call Count	The Dialer places calls to agents to reserve them for use while attempting to contact available customers. This counter tracks how many reservation calls were placed today.
Y	Answering Machine Call Count	A campaign can be enabled to differentiate between live voice and answering machines. This counter tracks how many answering machines were detected today.
Y	Customer Answered Call Count	A campaign can be enabled to differentiate between live voice and answering machines. If answering machine detection (AMD) is enabled for a campaign this counter increments when live voice is detected. If AMD is disabled, then all connected calls that are not FAX are identified as live voice. Direct Preview calls are identified as voice or AMD by the agent. This counter is reset daily at midnight.
Y	Customer Not Answered Call Count	The Dialer attempts to contact customers. This counter tracks how many attempts resulted in no answer condition. This counter is reset daily.
Y	Error Call Count	The Dialer attempts to contact customers. This counter tracks how many attempts resulted in a network error condition which includes no ring-back, no dial tone, and call disconnected from the network before ring no answer time out was exceeded.
Y	Number of attempted calls per second	This counter tracks how many calls per second the Dialer is placing rounded to the nearest integer. If the dialing rate is too high, it can result in network congestion on the voice network that can result in inefficient dialing.

Message Delivery Service

Performance Object

Cisco ICM MDSCLIENT

Counter Instance

“{Instance Name}”

Table 34: MDS Client Counters

Always ON?	Counter Name	Description
N	Client Handle ID	Handle for this MDS client. It is used to uniquely identify the MDS client connected to the MDS process.
N	Now Message Received	Number of messages received by the MDS client per second.
N	Now Message Sent	Number of messages sent by the MDS client per second.
N	Now Bytes Received	Number of bytes received by the MDS client per second.
N	Now Bytes Sent	Number of bytes sent by the MDS client per second

Always ON?	Counter Name	Description
N	Current Buffers Memory Allocated	Total number of bytes used by all currently allocated buffers.
N	Current Buffers Allocated	Total number of buffers currently allocated from buffer pool.
N	Buffers Allocation Requests/sec	Number of buffers allocated per second.
N	Buffers Free Requests/sec	Number of buffers freed per second.
N	Current Buffers Memory Limit	Maximum amount of memory allowed to be allocated for buffers for this process.
N	Initial Buffers Memory Limit	Amount of memory limit reserved for buffers for this process.
N	SendClientQ Current Depth	Current number of messages in the MDS Client Send Queue.
N	SendClientQ Now Messages In/sec	Total number of messages added to the MDS Client Send Queue per second.
N	SendClientQ Now Messages Out/sec	Total number of messages removed from the MDS Client Send Queue per second.
N	SendClientQ Now Bytes In/sec	Total number of bytes added for all messages to the MDS Client Send Queue per second.
N	SendClientQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the MDS Client Send Queue per second.
N	SendClientQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the MDS Client Send Queue per second.
N	SendClientQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the MDS Client Send Queue.
N	SendClientQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the MDS Client Send Queue experience.

Performance Object

Cisco ICM MDSPROCCLIENT

Counter Instance

“{Instance name}”

Table 35: MDS Process Client Counters

Always ON?	Counter Name	Description
N	Client Handle ID	Handle for this MDS client. It is used to uniquely identify the MDS client connected to the MDS process.
N	Total MDS Client Connects	Total number of times the MDS client has connected to the MDS process.
N	Total MDS Client Disconnects	Total number of times the MDS client has disconnected from the MDS process.
N	Now Message Received from Client	Number of messages received from the MDS client per second.

Always ON?	Counter Name	Description
N	Now Message Sent to Client	Number of messages sent to the MDS client per second.
N	Now Bytes Received from Client	Number of bytes received from the MDS client per second.
N	Now Bytes Sent to Client	Number of bytes sent to the MDS client per second.
N	ToClientQ Current Depth	Current number of messages in the MDS Send Client Queue.
N	ToClientQ Now Messages In/sec	Total number of messages added to the MDS Client Send Queue per second.
N	ToClientQ Now Messages Out/sec	Total number of messages removed from the MDS Client Send Queue per second.
N	ToClientQ Now Bytes In/sec	Total number of bytes added for all messages to the MDS Client Send Queue per second.
N	ToClientQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the MDS Client Send Queue per second.
N	ToClientQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the MDS Client Send Queue per second.
N	ToClientQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the MDS Client Send Queue.
N	ToClientQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the MDS Client Send Queue experience.

Performance Object

Cisco ICM MDSPROC

Counter Instance

“{Instance Name}”

Table 36: MDS Process Counters

Always ON?	Counter Name	Description
N	Current Buffers Memory Allocated	Total number of bytes used by all currently allocated buffers.
N	Current Buffers Allocated	Total number of buffers currently allocated from buffer pool.
N	Buffers Allocation Requests/sec	Number of buffers allocated per second.
N	Buffers Free Requests/sec	Number of buffers freed per second.
N	Current Buffers Memory Limit	Maximum amount of memory allowed to be allocated for buffers for this process.
N	Initial Buffers Memory Limit	Amount of memory limit reserved for buffers for this process.
N	Synch Messages Ordered/sec	Number of messages ordered by the MDS synchronizer per second.

Always ON?	Counter Name	Description
N	Synch MDS Duplicates/sec	Number of duplicate MDS messages detected by the synchronizer per second.
N	Synch DMP Duplicates/sec	Number of duplicate DMP messages detected by the synchronizer per second.
N	LocalHighInQ Current Depth	Current number of messages in the Local High Incoming Queue.
N	LocalHighInQ Now Messages In/sec	Total number of messages added to the Local High Incoming Queue per second.
N	LocalHighInQ Now Messages Out/sec	Total number of messages removed from the Local High Incoming Queue per second.
N	LocalHighInQ Now Bytes In/sec	Total number of bytes added for all messages to the Local High Incoming Queue per second.
N	LocalHighInQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Local High Incoming Queue per second.
N	LocalHighInQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Local High Incoming Queue per second.
N	LocalHighInQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Local High Incoming Queue.
N	LocalHighInQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Local High Incoming Queue experience.
N	LocalMedInQ Current Depth	Current number of messages in the Local Medium Incoming Queue.
N	LocalMedInQ Now Messages In/sec	Total number of messages added to the Local Medium Incoming Queue per second.
N	LocalMedInQ Now Messages Out/sec	Total number of messages removed from the Local Medium Incoming Queue per second.
N	LocalMedInQ Now Bytes In/sec	Total number of bytes added for all messages to the Local Medium Incoming Queue per second.
N	LocalMedInQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Local Medium Incoming Queue per second.
N	LocalMedInQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Local Medium Incoming Queue per second.
N	LocalMedInQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Local Medium Incoming Queue.
N	LocalMedInQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Local Medium Incoming Queue experience.

Always ON?	Counter Name	Description
N	LocalLowInQ Current Depth	Current number of messages in the Local Low Incoming Queue.
N	LocalLowInQ Now Messages In/sec	Total number of messages added to the Local Low Incoming Queue per second.
N	LocalLowInQ Now Messages Out/sec	Total number of messages removed from the Local Low Incoming Queue per second.
N	LocalLowInQ Now Bytes In/sec	Total number of bytes added for all messages to the Local Low Incoming Queue per second.
N	LocalLowInQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Local Low Incoming Queue per second.
N	LocalLowInQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Local Low Incoming Queue per second.
N	LocalLowInQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Local Low Incoming Queue.
N	LocalLowInQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Local Low Incoming Queue experience.
N	RemoteHighOutQ Current Depth	Current number of messages in the Remote High Output Queue.
N	RemoteHighOutQ Now Messages In/sec	Total number of messages added to the Remote High Output Queue per second.
N	RemoteHighOutQ Now Messages Out/sec	Total number of messages removed from the Remote High Output Queue per second.
N	RemoteHighOutQ Now Bytes In/sec	Total number of bytes added for all messages to the Remote High Output Queue per second.
N	RemoteHighOutQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Remote High Output Queue per second.
N	RemoteHighOutQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Remote High Output Queue per second.
N	RemoteHighOutQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Remote High Output Queue.
N	RemoteHighOutQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Remote High Output Queue experience.
N	RemoteMedOutQ Current Depth	Current number of messages in the Remote Medium Output Queue.
N	RemoteMedOutQ Now Messages In/sec	Total number of messages added to the Remote Medium Output Queue per second.

Always ON?	Counter Name	Description
N	RemoteMedOutQ Now Messages Out/sec	Total number of messages removed from the Remote Medium Output Queue per second.
N	RemoteMedOutQ Now Bytes In/sec	Total number of bytes added for all messages to the Remote Medium Output Queue per second.
N	RemoteMedOutQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Remote Medium Output Queue per second.
N	RemoteMedOutQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Remote Medium Output Queue per second.
N	RemoteMedOutQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Remote Medium Output Queue.
N	RemoteMedOutQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Remote Medium Output Queue experience.
N	RemoteLowOutQ Current Depth	Current number of messages in the Remote Low Output Queue.
N	RemoteLowOutQ Now Messages In/sec	Total number of messages added to the Remote Low Output Queue per second.
N	RemoteLowOutQ Now Messages Out/sec	Total number of messages removed from the Remote Low Output Queue per second.
N	RemoteLowOutQ Now Bytes In/sec	Total number of bytes added for all messages to the Remote Low Output Queue per second.
N	RemoteLowOutQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Remote Low Output Queue per second.
N	RemoteLowOutQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Remote Low Output Queue per second.
N	RemoteLowOutQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Remote Low Output Queue.
N	RemoteLowOutQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Remote Low Output Queue experience.
N	LocalHighOrderQ Current Depth	Current number of messages in the Local High Order Queue.
N	LocalHighOrderQ Now Messages In/sec	Total number of messages added to the Local High Order Queue per second.
N	LocalHighOrderQ Now Messages Out/sec	Total number of messages removed from the Local High Order Queue per second.
N	LocalHighOrderQ Now Bytes In/sec	Total number of bytes added for all messages to the Local High Order Queue per second.

Always ON?	Counter Name	Description
N	LocalHighOrderQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Local High Order Queue per second.
N	LocalHighOrderQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Local High Order Queue per second.
N	LocalHighOrderQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Local High Order Queue.
N	LocalHighOrderQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Local High Order Queue experience.
N	LocalMedOrderQ Current Depth	Current number of messages in the Local Medium Order Queue.
N	LocalMedOrderQ Now Messages In/sec	Total number of messages added to the Local Medium Order Queue per second.
N	LocalMedOrderQ Now Messages Out/sec	Total number of messages removed from the Local Medium Order Queue per second.
N	LocalMedOrderQ Now Bytes In/sec	Total number of bytes added for all messages to the Local Medium Order Queue per second.
N	LocalMedOrderQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Local Medium Order Queue per second.
N	LocalMedOrderQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Local Medium Order Queue per second.
N	LocalMedOrderQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Local Medium Order Queue.
N	LocalMedOrderQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Local Medium Order Queue experience.
N	LocalLowOrderQ Current Depth	Current number of messages in the Local Low Order Queue.
N	LocalLowOrderQ Now Messages In/sec	Total number of messages added to the Local Low Order Queue per second.
N	LocalLowOrderQ Now Messages Out/sec	Total number of messages removed from the Local Low Order Queue per second.
N	LocalLowOrderQ Now Bytes In/sec	Total number of bytes added for all messages to the Local Low Order Queue per second.
N	LocalLowOrderQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Local Low Order Queue per second.
N	LocalLowOrderQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Local Low Order Queue per second.

Always ON?	Counter Name	Description
N	LocalLowOrderQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Local Low Order Queue.
N	LocalLowOrderQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Local Low Order Queue experience.
N	RemoteHighOrderQ Current Depth	Current number of messages in the Remote High Order Queue.
N	RemoteHighOrderQ Now Messages In/sec	Total number of messages added to the Remote High Order Queue per second.
N	RemoteHighOrderQ Now Messages Out/sec	Total number of messages removed from the Remote High Order Queue per second.
N	RemoteHighOrderQ Now Bytes In/sec	Total number of bytes added for all messages to the Remote High Order Queue per second.
N	RemoteHighOrderQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Remote High Order Queue per second.
N	RemoteHighOrderQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Remote High Order Queue per second.
N	RemoteHighOrderQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Remote High Order Queue.
N	RemoteHighOrderQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Remote High Order Queue experience.
N	RemoteMedOrderQ Current Depth	Current number of messages in the Remote Medium Order Queue.
N	RemoteMedOrderQ Now Messages In/sec	Total number of messages added to the Remote Medium Order Queue per second.
N	RemoteMedOrderQ Now Messages Out/sec	Total number of messages removed from the Remote Medium Order Queue per second.
N	RemoteMedOrderQ Now Bytes In/sec	Total number of bytes added for all messages to the Remote Medium Order Queue per second.
N	RemoteMedOrderQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Remote Medium Order Queue per second.
N	RemoteMedOrderQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Remote Medium Order Queue per second.
N	RemoteMedOrderQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Remote Medium Order Queue.

Always ON?	Counter Name	Description
N	RemoteMedOrderQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Remote Medium Order Queue experience.
N	RemoteLowOrderQ Current Depth	Current number of messages in the Remote Low Order Queue.
N	RemoteLowOrderQ Now Messages In/sec	Total number of messages added to the Remote Low Order Queue per second.
N	RemoteLowOrderQ Now Messages Out/sec	Total number of messages removed from the Remote Low Order Queue per second.
N	RemoteLowOrderQ Now Bytes In/sec	Total number of bytes added for all messages to the Remote Low Order Queue per second.
N	RemoteLowOrderQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Remote Low Order Queue per second.
N	RemoteLowOrderQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Remote Low Order Queue per second.
N	RemoteLowOrderQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Remote Low Order Queue.
N	RemoteLowOrderQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Remote Low Order Queue experience.
N	TDHighQ Current Depth	Current number of messages in the Timed Delivery High Queue.
N	TDHighQ Now Messages In/sec	Total number of messages added to the Timed Delivery High Queue per second.
N	TDHighQ Now Messages Out/sec	Total number of messages removed from the Timed Delivery High Queue per second.
N	TDHighQ Now Bytes In/sec	Total number of bytes added for all messages to the Timed Delivery High Queue per second.
N	TDHighQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Timed Delivery High Queue per second.
N	TDHighQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Timed Delivery High Queue per second.
N	TDHighQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Timed Delivery High Queue.
N	TDHighQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Timed Delivery High Queue experience.
N	TDMedQ Current Depth	Current number of messages in the Timed Delivery Medium Queue.
N	TDMedQ Now Messages In/sec	Total number of messages added to the Timed Delivery Medium Queue per second.

Always ON?	Counter Name	Description
N	TDMedQ Now Messages Out/sec	Total number of messages removed from the Timed Delivery Medium Queue per second.
N	TDMedQ Now Bytes In/sec	Total number of bytes added for all messages to the Timed Delivery Medium Queue per second.
N	TDMedQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Timed Delivery Medium Queue per second.
N	TDMedQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Timed Delivery Medium Queue per second.
N	TDMedQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Timed Delivery Medium Queue.
N	TDMedQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Timed Delivery Medium Queue experience.
N	TDLowQ Current Depth	Current number of messages in the Timed Delivery Low Queue.
N	TDLowQ Now Messages In/sec	Total number of messages added to the Timed Delivery Low Queue per second.
N	TDLowQ Now Messages Out/sec	Total number of messages removed from the Timed Delivery Low Queue per second.
N	TDLowQ Now Bytes In/sec	Total number of bytes added for all messages to the Timed Delivery Low Queue per second.
N	TDLowQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Timed Delivery Low Queue per second.
N	TDLowQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Timed Delivery Low Queue per second.
N	TDLowQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Timed Delivery Low Queue.
N	TDLowQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Timed Delivery Low Queue experience.
N	Output Waits	Total number of times output from critical client (Route or OPC) waited for ACK from MDS peer.
N	Average Output Wait Time	Average number of milliseconds MDS output waits to receive an ACK message from MDS peer.
N	Private Net Min RTT	Minimum time it took MDS to send a message over the private network and receive an ACK response from MDS peer.
N	Private Net Avg RTT	Average time it took MDS to send a message over the private network and receive an ACK response from MDS peer.
N	Private Net Max RTT	Maximum time it took MDS to send a message over the private network and receive an ACK response from MDS peer.

Enable optional counters

To enable Windows PerfMon counter reporting for the Message Delivery Service, you must add a new registry value (EnablePerformanceMonitor) to enable MDS process and MDS client counters.

For the MDS process, the value is created under the MDS Process key

Key
 HKEY_LOCAL_MACHINE_SOFTWARE\Cisco Systems,
 Inc.\ICM*<Instance>*\<node>\MDS\CurrentVersion\Process

Name
 EnablePerformanceMonitor

Type
 REG_DWORD

Default
 0 (disabled)

Enabled
 1

For MDS clients, the value is created under each client key

Key
 HKEY_LOCAL_MACHINE_SOFTWARE\Cisco Systems,
 Inc.\ICM*<Instance>*\<node>\MDS\CurrentVersion\Clients*<client>*

Name
 EnablePerformanceMonitor

Type
 REG_DWORD

Default
 0 (disabled)

Enabled
 1



Note A change in this registry key is immediately detected. Performance monitor counters become enabled or disabled within 10 seconds. When Performance Monitor reporting is enabled for the MDS process, no statistical metering is reported to the MDS process log file due to overlapping functionality. When PerfMon reporting is disabled, statistical metering reporting resumes.

QoS

Performance Object

Cisco ICM QoS

Counter Instance

“{Instance Name}”

Table 37: Cisco ICM QoS

Always ON?	Counter Name	Description
N	High BytesSent/sec	High BytesSent/sec is the number of bytes per second sent to the other side over high priority connection.

Always ON?	Counter Name	Description
N	High MsgsSent/sec	High MsgsSent/sec is the number of messages sent to the other side over high priority connection.
N	High BytesRcvd/sec	High BytesRcvd/sec is the number of bytes received from the other side over high priority connection.
N	High MsgsRcvd/sec	High MsgsRcvd/sec is the number of messages received from the other side over high priority connection.
N	High LocalRttMean	High LocalRttMean is the mean Round Trip Time in milliseconds of high priority messages as measured by local node.
N	High LocalRttStdDev	High LocalRttStdDev is the standard deviation of Round Trip Time of high priority messages as measured by local node.
N	High RemoteRttMean	High RemoteRttMean is the mean Round Trip Time in milliseconds of high priority messages as measured by remote node.
N	High RemoteRttStdDev	High RemoteRttStdDev is the standard deviation of Round Trip Time of high priority messages as measured by remote node.
N	High Xmit NowQueueDepth	High Xmit NowQueueDepth is the current number of messages in the transmit queue for high priority traffic.
N	High Xmit MaxQueueDepth	High Xmit MaxQueueDepth is the maximum number of message observed in the transmit queue for high priority traffic.
N	High Xmit NowBytesQueued	High Xmit NowBytesQueued is the current number of bytes in the retransmit queue for high priority traffic.
N	High Xmit MaxBytesQueued	High Xmit MaxBytesQueued is the maximum number of bytes observed in the retransmit queue for high priority traffic.
N	High TotalQoSReallocations	High TotalQoSReallocations is the total number of times QoS resources had to be reallocated for high priority connection because usage has exceeded previous allocation over defined threshold levels.
N	Med BytesSent/sec	Med BytesSent/sec is the number of bytes per second sent to the other side over medium priority connection.
N	Med MsgsSent/sec	Med MsgsSent/sec is the number of messages sent to the other side over medium priority connection.
N	Med BytesRcvd/sec	Med BytesRcvd/sec is the number of bytes received from the other side over medium priority connection.
N	Med MsgsRcvd/sec	Med MsgsRcvd/sec is the number of messages received from the other side over medium priority connection.
N	Med LocalRttMean	Med LocalRttMean is the mean Round Trip Time in milliseconds of medium priority messages as measured by local node.
N	Med LocalRttStdDev	Med LocalRttStdDev is the standard deviation of Round Trip Time of medium priority messages as measured by local node.
N	Med RemoteRttMean	Med RemoteRttMean is the mean Round Trip Time in milliseconds of medium priority messages as measured by remote node.

Always ON?	Counter Name	Description
N	Med RemoteRttStdDev	Med RemoteRttStdDev is the standard deviation of Round Trip Time of medium priority messages as measured by remote node.
N	Med Xmit NowQueueDepth	Med Xmit NowQueueDepth is the current number of messages in the transmit queue for medium priority traffic.
N	Med Xmit MaxQueueDepth	Med Xmit MaxQueueDepth is the maximum number of message observed in the transmit queue for medium priority traffic.
N	Med Xmit NowBytesQueued	Med Xmit NowBytesQueued is the current number of bytes in the retransmit queue for medium priority traffic.
N	Med Xmit MaxBytesQueued	Med Xmit MaxBytesQueued is the maximum number of bytes observed in the retransmit queue for medium priority traffic.
N	Med TotalQoSReallocations	Med TotalQoSReallocations is the total number of times QoS resources had to be reallocated for medium priority connection because usage has exceeded previous allocation over defined threshold levels.
N	Low BytesSent/sec	Low BytesSent/sec is the number of bytes per second sent to the other side over low priority connection.
N	Low MsgsSent/sec	Low MsgsSent/sec is the number of messages sent to the other side over low priority connection.
N	Low BytesRcvd/sec	Low BytesRcvd/sec is the number of bytes received from the other side over low priority connection.
N	Low MsgsRcvd/sec	Low MsgsRcvd/sec is the number of messages received from the other side over low priority connection.
N	Low LocalRttMean	Low LocalRttMean is the mean Round Trip Time in milliseconds of low priority messages as measured by local node.
N	Low LocalRttStdDev	Low LocalRttStdDev is the standard deviation of Round Trip Time of low priority messages as measured by local node.
N	Low RemoteRttMean	Low RemoteRttMean is the mean Round Trip Time in milliseconds of low priority messages as measured by remote node.
N	Low RemoteRttStdDev	Low RemoteRttStdDev is the standard deviation of Round Trip Time of low priority messages as measured by remote node.
N	Low Xmit NowQueueDepth	Low Xmit NowQueueDepth is the current number of messages in the transmit queue for low priority traffic.
N	Low Xmit MaxQueueDepth	Low Xmit MaxQueueDepth is the maximum number of message observed in the transmit queue for low priority traffic.
N	Low Xmit NowBytesQueued	Low Xmit NowBytesQueued is the current number of bytes in the retransmit queue for low priority traffic.
N	Low Xmit MaxBytesQueued	Low Xmit MaxBytesQueued is the maximum number of bytes observed in the retransmit queue for low priority traffic.
N	Low TotalQoSReallocations	Low TotalQoSReallocations is the total number of times QoS resources had to be reallocated for low priority connection because usage has exceeded previous allocation over defined threshold levels.

Enable Optional Counters

Because there is overhead in maintaining QoS Performance Monitoring counters, the performance monitoring feature is turned off by default. To enable this feature, change the following registry key value to 1 and cycle the application process.

Key

```
HKEY_LOCAL_MACHINE_SOFTWARE\Cisco Systems,  
Inc.\ICM\<Instance>\<node>\DMP\CurrentVersion
```

Name

EnablePerformanceMonitor

Type

REG_DWORD

Default

0 (disabled)

Enable

1



Note The amount of overhead is dependent on the periodic update interval. This interval should be set reasonably high to minimize the impact on the system.



CHAPTER 8

Capacity Planning

- [Capacity Planning Process](#), on page 141
- [Capacity Planning – Getting Started](#), on page 142
- [Collected Data Categorization](#), on page 143
- [Capacity Utilization](#), on page 146

Capacity Planning Process

Figure 25: Capacity Planning Process



Change an existing Unified ICM/Unified CCE deployment in small steps. Then analyze the impact of each step with a well-established, repeatable process. This process includes the following phases (steps):

1. **Sample Phase:** Start data sampling at the same time for the same interval for each change made.
2. **Collect and Categorize Phase:** Collect the samples and distribute to appropriate buckets.
3. **Analysis Phase:** Check application resource boundaries – has any component exceeded utilization limits? Determine best fit for new deployment requirements. Estimate solution level capacity utilization for new requirements.
4. **Change Phase:** Implement changes to solution based on analysis and estimate of impact.
5. **Do it all over again.** Run the process again in the same way as before to ensure that a proper comparison is made.

Capacity Planning – Getting Started

The first thing you must do to get started with a capacity management plan is to establish a baseline – answer the question: “what is my capacity utilization today?” To answer this question, you must first determine the busiest, recurring period within a reasonable timeframe. For most business call centers, there is usually a 1-hour period of each day that is typically the busiest. Moreover, there can be busier days of the week (for example Monday vs. Wednesday); busier days of the month (last business day of the month) or busier weeks of the year (for example, the first week in January for insurance companies, or for the IRS, the first two weeks of April). These traditionally busy hours, days, or weeks represent the most taxing period on the deployment; these are the periods during which a capacity utilization calculation is best because you always want to ensure that your deployment is capable of handling the worst.

The steps to getting started are:

1. Set up basic sampling (daily)

Sample the performance counter values: CPU, Memory, Disk, Network, Call and Agent Traffic

2. Determine the busy period

Identify the recurring busy period – worst case scenario – by:

Per Component

Solution Wide

3. Establish a baseline of utilization for the target period

Determine hardware capacity utilization

Identify components with high capacity utilization

4. Craft a recurring collection plan

Devise a plan that is repeatable – such as automated – that can be done on a weekly basis whereby samples are obtained during the busiest hour of the week.

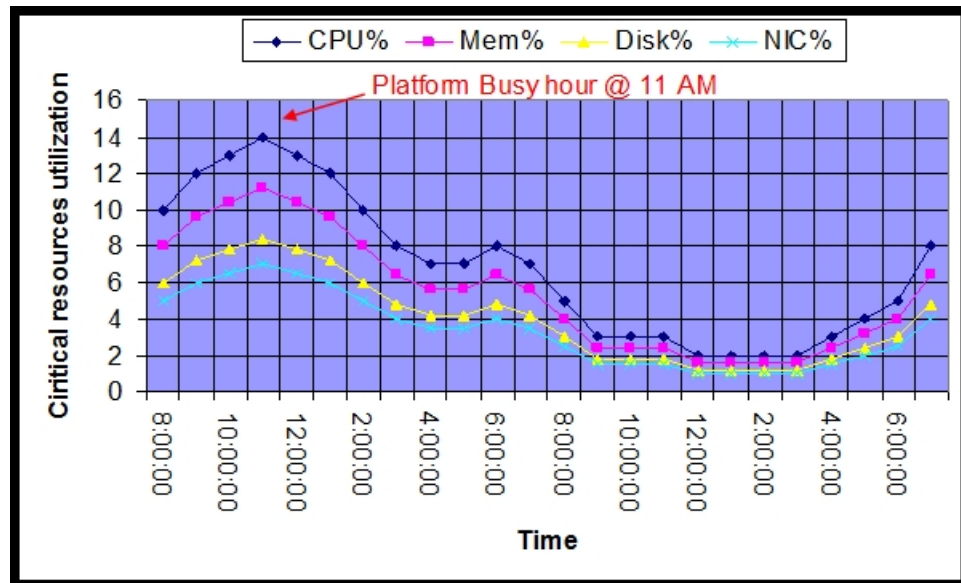
After you establish a baseline and identify a busy hour, daily sampling is no longer necessary; you must sample only during the busy hour on a weekly basis. However, if regular reporting shows that the busy hour may have changed, then you must complete daily sampling again so that you can identify the new busy hour. After you identify the new busy hour, weekly sampling during the busy hour can resume.

Finding the Busy Hour

To find the busy hour, start continuous data sampling to cover a full week, 24 hours a day. The data sampled are the performance counters for CPU, Memory, Disk, and Network as listed in [Capacity Utilization, on page 146](#). You can set up performance counter values to be written to a disk file in comma-separated values (.CSV) format, which is easily imported into a Microsoft Excel workbook. Collect the data sample files, import them into Excel and graph them to see the busy hour. You can import the data set into a graph in a matter of minutes and easily determine the busy hour.

For example:

Figure 26: Graph of Samples to Find Busy Hour



Collected Data Categorization

Collected data should be categorized by critical resource for each change event or need. The list below shows the instigators for sampling, collecting, categorizing, analyzing data to determine capacity utilization.

- Current Deployment Design
- Configuration Info
- Traffic Load
- Migration Requirements
- Platform Performance

Current Deployment Design

Establish and maintain a deployment baseline. This baseline is used to do before and after comparisons. Establish a new baseline after you change the deployment design.

- Establish an initial baseline – today – with the current deployment design
- Re-establish a baseline after deployment changes occur, such as:
 - Add or delete a Peripheral Gateway
 - Add or delete an Administration & Data Server
 - Clustering over WAN – any change to WAN characteristics

You can use week-to-week comparisons to identify changes that occurred that you were not aware of. For example, someone adds more skill groups without prior approval or notification and suddenly utilization jumps, inexplicably, by 5%. Such a change is noteworthy enough to ask the following questions: What changed? When? Why?

When analyzing the current solution, maintain deployment information and track changes:

- Topology diagrams (network)
- Peripheral counts
 - Cisco Unified Communications Manager Clusters
 - Unified IP-IVR or Unified CVP peripherals (and port quantity)
- Network devices
- Third-party add ons

Configuration Information

Changes to Unified ICM/Unified CCE configuration can impact computing resources and thus impact the utilization for a hardware platform, an application component and in some cases, the entire solution.

Configuration change examples:

- Adding skill groups
- Changing number of skill groups per agent
- Adding ECC data
- Increasing calls offered (per peripheral) per half hour

Using the baseline that you established, you can characterize the impact of the configuration change by comparing utilization before the change to utilization after change.

By making changes methodically in small steps, you can characterize each small change (for example, adding one skill group at a time) and note the impact. In the future, if a change request comes to add 10 skills group, you can make an educated guess at the overall utilization impact by extrapolating: adding one skill group caused a 0.5% increase in PG CPU utilization at the half hour, so adding 10 skill groups can result in a 5% increase in PG CPU utilization at the half hour. Can a 5% increase in PG CPU utilization be accommodated?

Configuration changes often have an impact on performance. Ensure that you track ongoing changes and analyze the impact. The following configuration changes are likely to impact utilization:

- Overall Database Size
- Number of Skill Groups per Agent
- Number of Skill Groups per Peripheral
- Number of Call Types
- Number of Dialed Numbers
- Number of Agents per Peripheral
- Total Agent Count
- Amount of Attached Call Data

Other configuration factors that can affect utilization:

- Agent level reporting
- Persistent ECC, per call type, per peripheral
- Percentage of call types per peripheral
- Average skill group per agents and total skills per system
- Number of Administration & Data Servers (real time feeds)
- Number of concurrent reporting users

Traffic Load

Examples of impacting traffic load changes:

- **Inbound call rate**

For example, your marketing department is about to introduce a new discount program for an existing service: “Sign up before July 31 for the new discounted rate!” You have been monitoring inbound call rate (Unified ICM/Unified CCE Router: Calls/sec counter) and see a relatively consistent 4 calls/sec inbound rate during the Monday morning busy hour as compared to an average of 3 calls/sec during the rest of the day. You predict that the new marketing program will increase the inbound call rate to 6 calls per second during the busy hour. You calculated that utilization is at 50% during the busy hour while averaging at 40% during the rest of the day. You determine that the increase in call rate will push utilization as high as 75%, which the system can tolerate.

- **Network utilization**

The Unified ICM/Unified CCE system is a collection of distributed, dependent software components that communicate by network messaging. Components communicate via a public network connection – some components also communicate via a private, dedicated network connection. On the public network, the Unified ICM/Unified CCE may be competing for network bandwidth. Any increase in public network utilization may slow the ability of a Unified ICM/Unified CCE component to transmit data on the network, causing output queues to grow more than the usual values. This can impact memory utilization on the server and timing of real-time operations.

Any change in traffic or load has a corresponding impact on utilization and capacity. Additional examples of impacting traffic include:

- Overall Call Load—BHCA and Calls per Second
- Persistent ECC, per call type, per peripheral
- Percentage of call types per peripheral
- Number of concurrent agents logged in (including monitored IVR ports)
- Number of concurrent reporting users

Migration Requirements

When analyzing future growth, you must consider all possible migrations:

- Business requirements for migration: Adding a new line of business, additional skill groups
- Expected growth: Recent history has shown a steady 10% increase in agent population
- Resource consolidations or separations:
 - Agents
 - Call Types
 - Reporting
 - Queuing
 - Merging two peripherals into one
- Other requirements:
 - Office moving to new location
 - Network infrastructure change: increased/decrease network latency
 - Splitting PG sides over WAN

- Changing data retention parameters on the HDS

Platform Performance

Any hardware or software changes in the platform itself can have a corresponding impact on utilization.

A “technology refresh” upgrade (upgrading both hardware and software) of the Unified ICM/Unified CCE has a significant effect on capacity utilization. Advances in hardware capabilities and a continued focus on streamlining bottlenecks in the software have yielded significant increases in server and component capacities.

In some cases, hardware upgrades (without a software upgrade) may be necessary to accommodate growth in the Unified ICM/Unified CCE deployment.

A “common ground” upgrade (upgrading software while retaining existing hardware) of Unified ICM/Unified CCE may have a differing effect on capacity utilization depending on the changes made to the software from one release to the next. In some components, utilization may increase slightly because new functionality was added to the component, which has slightly decreased its performance. However, another component in which performance improvements was introduced, utilization may decrease from one release to the next.

You must plan to re-establish a capacity utilization baseline after any upgrade.

Capacity Utilization

Platform resource utilization data is at the foundation of capacity analysis. This data is sampled values of performance counters such as: CPU, Memory, Disk, and Network. The data set is from the busy hour as determined by the steps described above.

To eliminate short-duration spikes that are statistical outliers, use a sample rate of one sample every 15 seconds of each of the listed counters. Of the sample set, base the calculation on the 95th percentile sample. The 95th percentile is the smallest number that is greater than 95% of the numbers in a given set.

Counters are divided into two categories:

- “Measurement” value:

A measurement value is only valid if the indicator values are “good.” If the indicator values are within acceptable levels, then the measurement value is used in the forthcoming calculation to determine utilization.

- “Indicator” value:

An indicator value is a Boolean indication of “good” or “bad” – exceeding the maximum threshold is, of course, “bad.” If the indicator value is “bad,” assume that capacity utilization was exceeded. If so, you must take steps to return the system to < 100% utilization which may require hardware upgrade.

Capacity utilization is considered to be $\geq 100\%$ if published sizing limits are exceeded for any given component. See the *Cisco Unified Contact Center Enterprise Design Guide* at https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html for a quick reference on configuration limits and scalability constraints. For more information see [Unified Communications in a Virtualized Environment](#).

For information on *Contact Center Enterprise Compatibility Matrix* see <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html>.

For information on system constraints, see the [Unified Communications Sizing Tool](#). For example: if the server on which a Unified CC PG is installed has a published capacity of 1,000 agents but there are 1,075 active agents at a particular time, the server is considered to be greater than 100% utilization regardless of what might be calculated using the methods described herein. The reason for this is that although the server/application seems to be performing at acceptable levels, any legitimate change in usage patterns could drive utilization beyond 100% and cause a system outage because the published capacity was exceeded. Published capacities seek to take into account differences between deployments and/or changes in usage patterns without driving the server into the red zones of performance thresholds. As such, all deployments must remain within these published capacities to enjoy continued Cisco support.

CPU Utilization Calculations

Table 38: Calculating CPU Utilization

$\overline{CPU}_{\rho}(t_n) = \frac{CPU_{95\%}(t_n)}{CPU_{Sat}} * 100$	
CPU _{95%}	Measurement Counter: Processor – % Processor Time (_Total)
CPU _{Sat}	Maximum threshold: 60%
Indicator Counter	Counter: System – Processor Queue Length Threshold: 2 X # CPU Cores

Memory Utilization Calculations

Table 39: Calculating Memory Utilization

$Mem_{Sat} = Mem_{physical} * .8$ $\overline{Mem}_{\rho}(t_n) = \frac{Mem_{95\%}(t_n)}{Mem_{Sat}} * 100$	
Mem _{95%}	Measurement Counter: Memory – Committed Bytes
Mem _{Sat}	Threshold: 80% (of physical memory)
Indicator Counters	Counter: Memory – Available Mbytes Threshold: < 20% Counter: Memory – Memory – Pages / sec Threshold: 20% Counter: Paging File – % Usage Threshold: 80%

Disk Utilization Calculations

Table 40: Calculating Disk Utilization

$\overline{Disk}_{\rho}(t_n) = \frac{DT_{95\%}(t_n)}{DT_{Sat}} * 100$	
DT _{95%}	Measurement Counter: Processor – % Processor Time (_Total)
DT _{Sat}	Maximum threshold: 50%
Indicator	Counter: Physical Disk – Avg. Disk Queue Length Threshold: 1.5

NIC Utilization Calculations

Table 41: Calculating NIC Utilization

$NIC_{Sat} = NIC_{physical} * .03$ $\overline{NIC}_{\rho}(t_n) = \frac{NIC_{95\%}(t_n)}{NIC_{Sat}} * 100$	
NIC _{95%}	Measurement Counter: Network Interface – Bytes Total / sec
NIC _{Sat}	Maximum threshold: 30% 100 Mbps NIC: 3 MB / sec (approximately) 1 Gbps NIC: 30 MB / sec (approximately)
Indicator	Counter: Network Interface – Output Queue Length Threshold: 1

Maximum Utilization Calculations

The highest utilization can be determined with

$$\overline{UTIL}_{\rho} = MAX(\overline{CPU}_{\rho}[t], \overline{Mem}_{\rho}[t], \overline{Disk}_{\rho}[t], \overline{NIC}_{\rho}[t])$$

Relating Traffic Load to Resources

Use Unified ICM/Unified CCE Router counters to relate traffic load to resource utilization. The Unified ICM/Unified CCE Router Performance Counters are:

- Calls/sec
- Calls In Progress

- Agents Logged On

Graphing these data sets relative to resource data sets may provide a compelling visual message.



CHAPTER 9

Diagnostic Tools

- [Diagnostic Framework](#), on page 151
- [CLI Configuration](#), on page 189
- [Diagnostic Framework API](#), on page 198
- [Diagnostic Framework Troubleshooting](#), on page 240
- [DUMPLOG](#), on page 241
- [EMSMON](#), on page 245
- [Unified CCE Certificate Monitoring Service](#), on page 247

Diagnostic Framework

Overview

Unified ICM/Unified CCE servers use the web-based Diagnostic Framework service to collect (and sometimes set) diagnostic information for that server. The Diagnostic Framework service is a REST-like service that accepts requests over HTTPS, gathers information from the system, and responds in the form of an XML response message. It can collect a variety of data, such as process logs, current trace values, network status, PerfMon values, and so on. You can also use the service to collect log files from the server. For a complete list of the capabilities, see [Diagnostic Framework API](#), on page 198.

You can use the Diagnostic Framework as follows:

- For Unified CCE deployments, the primary access method is through the Analysis Manager, which serves as a solution-wide serviceability portal.
- Unified CCE deployments can also use the Unified Communication diagnostic clients' CLI.
- Each Diagnostic Framework service also includes an HTML-based web user interface that provides access to the complete list of the API commands.
- The API can also be accessed directly through a browser.

For more information about how to access the service, see [Usage](#), on page 161.

Installation and Configuration

The Diagnostic Framework service is installed as part of the Unified ICM/Unified CCE software by the ICM-CCE installer (henceforth, called the Unified ICM installer). You require no additional installation or

configuration steps. You may optionally choose to customize the service if needed, such as change the port number, certificate, or logging level as explained in the following sections.

Service Registration and Dependencies

Diagnostic Framework is a .NET based web service. It is registered in the Windows service control by the Unified ICM installer.³ The service files are laid down under the following folder:

```
<ICM_Drive>:\icm\serviceability\diagnostics
```

You can start or stop the Diagnostic Framework service from the Windows service control panel.

The service is registered under the following name: “Cisco ICM Diagnostic Framework”

The Diagnostic Framework is hosted on top of the HTTP service built in the Windows Server kernel. It does not require IIS or any other web server to be installed. The Diagnostic Framework uses the Windows HTTP SSL service to provide secure communications between the server and the client. Therefore, enable the HTTP SSL service before starting the Diagnostic Framework service. The Unified ICM installer configures this dependency in the Windows service control panel to automatically start the HTTP SSL service when you start the Diagnostic Framework service.



Note Note: The Diagnostic Framework or HTTP SSL service does not require IIS. However, if IIS is installed, the HTTP SSL service adds a dependency on the IIS service. Therefore, for HTTP SSL and the Diagnostic Framework to work, start IIS.

Configure Service Port

The Diagnostic Framework listens on TCP port 7890.

You can change the port number. To change the port number, update the Diagnostic Framework service configuration file and the certificate registration with Windows. Change the port number on the CLI and Analysis Manager clients too. Also, change the port number on every other Unified ICM server where other instances of the Diagnostics Framework are running.



Note Consider changing the port number only if necessary.

Procedure

-
- Step 1** Stop Diagnostic Framework service through Windows service control.
 - Step 2** Open command prompt and change directory to

```
<ICM_Drive>:\icm\serviceability\diagnostics\bin
```
 - Step 3** Run **DiagFwCertMgr /task:ValidateCertBinding** command and confirm from output that certificate binding with current port is valid.
 For more information about the DiagFwCertMgr utility, see [Certificate Management, on page 159](#).
 - Step 4** Record thumbprint of certificate in use.

³ The Unified ICM installer detects and installs the appropriate .NET version.

You need the thumbprint to register the certificate with a different port. You can access it either from the output of the preceding command or from the following registry value: HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\Serviceability\DiagnosticFramework\CertUsedByDiagFwSvc

- Step 5** In same command window, run **DiagFwCertMgr /task:UnbindCert** command to remove certificate binding from current port.
- Step 6** Launch Notepad and open service configuration file
<ICM_Drive>:\icm\serviceability\diagnostics\bin\DiagFwSvc.exe.config
- Note** You may want to copy this configuration file before you change it.
- Step 7** Save file and quit Notepad.
- Step 8** Open command prompt and change directory to
<ICM_Drive>:\icm\serviceability\diagnostics\bin
- Step 9** Run **DiagFwCertMgr/task:BindCertFromStore/certhash:<hash of the certificate noted above>** command to bind the certificate to the new port number.
- The utility reads the port number from the service configuration file.
- Step 10** Read output and confirm that preceding command completed successfully.
- Step 11** (Optional) Run **DiagFwCertMgr/task:ValidateCertBinding** command again to verify changes to port number binding.
- Step 12** Restart Diagnostic Framework service.

What to do next

If you configured the Windows Firewall, make sure that the new port opened in the firewall configuration.

Enabling ECDSA

Before you begin

Installer generates self-signed ECDSA certificate, imports to the windows local store, and updates the ECDSA thumbprint registry at SOFTWARE\WOW6432Node\Cisco Systems, Inc.\ICM\Serviceability\DiagnosticFramework.

Procedure

- Step 1** In Windows service control, stop Diagnostic Framework service.
- Step 2** In the command prompt, change the directory to
<ICM_Drive>:\icm\serviceability\diagnostics\bin.
You have to remove the binding from the existing port.
- Step 3** Run the command **DiagFwCertMgr/task:UnbindCert** to remove the existing certificate binding from the current port. You can now bind the ECDSA certificate.
- Step 4** To bind the ECDSA certificate to the current port, run the command **DiagFwCertMgr /task:CreateAndBindCertECDSA**.

- Note** Certificate matching to the thumbprint of ECDSA registry will be used to bind the port.
- To remove ECDSA certificate, you can run the command **DiagFwCertMgr /task:UnbindAndDeleteCertECDSA**. This command will remove the certificate binding from the current port and will delete the self-signed ECDSA certificate created by the option **CreateAndBindCertECDSA**.
- Note** For more commands of ECDSA, refer, to the table *Diagnostic Framework Certificate Manager Utility Tasks* in the chapter *Diagnostic Tools* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html>

Installing or Updating Third-Party Certificate

During installation, the Diagnostic Framework generates a self-signed certificate with its name set to the server hostname. The self-signed certificate can be replaced with a trusted third-party signed certificate. For more information, see [Certificate Management, on page 159](#).

Diagnostic Framework Log Files and Logging Level

The Diagnostic Framework log files are created in the folder
`<ICM_Drive>:\icm\serviceability\diagnostics\logs.`

The Diagnostic Framework uses the industry-standard log4net library to create and manage its log files. A configuration file controls the names of the log files, how large they can get, how many rollover files are kept, the logging level, and so on.

The default logging level 'INFO' is sufficient for most cases. Do not change the logging level unless directed by the TAC.

You can change the log level by editing the file
`<ICM_Drive>:\icm\serviceability\diagnostics\config\log4net.config` and changing the `<level>` tag value to "DEBUG" (or "WARN," "ERROR," or "FATAL").

```
<root>
  <level value="INFO" />
  <appender-ref ref="RollingFileAppender" />
</root>
```

Diagnostic Framework Service Resources Requirements

Reduced Priority

The Diagnostic Framework service runs at a Below Normal priority to avoid adversely impacting server/application performance while running.

Changing Service CPU Threshold

Some CPU-intensive APIs of the Diagnostic Framework first check the overall system CPU utilization value (%CPU). These APIs do not start the request if the %CPU value is greater than a threshold value.

These APIs are:

- LogMgr commands

- TraceMgr commands
- ConfigMgr command

There are a few registry keys that control this behavior. Look in the following Windows Registry Key:

HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\Serviceability\DiagnosticFramework

Table 42: CPU Threshold

Registry key	Default Value	Description
CPUThresholdSample	5	To get a more accurate reading of the %CPU, multiple readings are taken. This value says how many samples should be read.
CPUThresholdDelay	2	The number of milliseconds to wait between each sample taken.
CPUThresholdPercent	60	The percent value to compare the current %CPU to. If the %CPU is greater than this value, the API cannot start. An error returns telling the user that the server is too busy, and to try the command later.

Change Maximum Number of Concurrent Requests

The Diagnostic Framework service is designed to handle up to 20 concurrent web requests. The system was tested under load to work with this configuration. However, if you must lower the number of concurrent requests, you can modify the value of `maxConcurrentCalls` property in the service configuration file.

Procedure

-
- Step 1** Stop Diagnostic Framework service.
- Step 2** Launch Notepad and open file
`<ICM_Drive>:\icm\serviceability\diagnostics\bin\DiagFwSvc.exe.config.`
- Tip** You may want to copy this configuration file before you change it.
- Step 3** Locate element `<serviceThrottling maxConcurrentCalls="20" />` and change value to any number below 20.
- Caution** Do not increase the value beyond 20. It may lead to unexpected results during peak call volume.
- Step 4** Save file and quit Notepad.
- Step 5** Restart Diagnostic Framework service.
-

Security

The Diagnostic Framework provides the infrastructure to establish a secure connection between the service and its clients. It uses HTTP form authentication over SSL to authenticate, authorize, and encrypt the connection. You need a valid Diagnostic Framework user account to access the service. Connections are not session oriented; the connection is maintained from the receipt of a request until the response is sent.

For service provider deployments, the Diagnostic Framework service is ICM instance aware, and can control access based on instance data requested.

Log In to the Diagnostic Framework Portico

To access the Diagnostic Framework Portico tool, do the following:

Before you begin

If your machine is in a domain, any user who is a local administrator and a domain user on the machine can login.

However, to view the lists and perform the tasks in the Diagnostic Framework Portico tool, you must be a local administrator on the machine *and* must be either a domain admin in the machine's domain or a member of at least one setup security group in the machine's domain.

If your machine is in a workgroup, you must be a local administrator.

Procedure

-
- Step 1** In your browser's address bar, type: `https://localhost:7890/icm-dp/DignosticPortal`.
 - Step 2** Press **Enter**.
The Login page appears.
 - Step 3** Enter your Active Directory username and password.
 - Step 4** Click **Log In**.
-

Log Out of the Diagnostic Framework Portico

For security purpose logout when you are finished using the Diagnostic Framework Portico tool. To log out, click **Log Out** at the top-right of the page. This returns you to the login page.



-
- Note** If no activity in which you contact the server occurs in a 30 minute period, you are automatically logged out. If a forced logout occurs, you must log in again to resume using the tool.
-

Authentication, Authorization, and Auditing

The Diagnostic Framework service integrates with Windows as well as Active Directory to provide user management and access control. The Diagnostic Framework allows two sets of users:

- *A local Windows user who is a member of the local Windows security group called `ICMDiagnosticFrameworkUsers` on the server where the service exists:* This group is created by the Unified ICM installer and is initially empty, so by default, no local users have access to the service. The administrator on the server can make any local user a member of this group and provide access to Diagnostic Framework service. To add a user to the `ICMDiagnosticFrameworkUsers` group, use the Computer Management tool under Administrative Tools.

- *A trusted domain user who is a member of local Administrators group on the server where the service exists:* A trusted domain user who is a member of local administrators on the server can make any trusted domain user a member of this group and provide access to Diagnostic Framework service.
- *A trusted domain user who is a member of local ICMDiagnosticFrameworkUsers group on the server where the service exists:* A trusted domain user who is a member of local administrators group on the server can make any trusted domain user a member of ICMDiagnosticFrameworkUsers group and provide access to Diagnostic Framework service.
- *A trusted domain user who is a member of the CONFIG domain security group of the Unified ICM/Unified CCE instance being accessed:* A Unified ICM/Unified CCE SETUP user or domain administrator can make any trusted user a member of the instance CONFIG group. Nested membership is allowed too; as a result the SETUP users and domain administrator can also access the service. To add a user to the instance CONFIG group use the Active Directory Users and Computers tool or Unified ICM/Unified CCE User List tool. Access to domain users is configurable. By default, all direct and nested members of the CONFIG group have access to the service. However, you can disable access to domain users as follows:
 1. Stop the Diagnostic Framework service.
 2. Launch Notepad and open the file
`<ICM_Drive>:\icm\serviceability\diagnostics\bin\DiagFwSvc.exe.config`



Tip Tip: You may want to make a copy of this configuration file before making any changes to it.

3. Locate the element `<add key="DomainAuthorizationEnabled" value="1" />` and change the value from 1 to 0
4. Save the file and quit Notepad.
5. Restart the Diagnostic Framework service.



Note A Diagnostic Framework user does not require administrative privileges on the server to access the service.

The user authentication, validating username and password, is managed by Windows or Active Directory. Therefore, all valid or invalid sign in attempts are logged in the Windows Event Viewer (provided that login/logout auditing is enabled). The user authorization, validating group membership and optionally Unified ICM instance access, is managed by the Diagnostic Framework service. Hence, all authorization requests can be audited through the Diagnostic Framework logs.



Note A user may be a valid Windows or Active Directory user but may not be a member of the required security groups for access to Diagnostic Framework service. As a result, even though the user may pass authentication, it may not pass authorization.

Because the Diagnostic Framework user is managed by Windows or by Active Directory, the user is subjected to the password policies of the server or the domain. Always set strong password policies. For more information

about system hardening and password policies, see the *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html>.

Special Consideration for Servers with Multiple Unified ICM Instances

This section applies to environments similar to service providers, who have multiple Unified ICM instances on each server.

The domain user is authorized against the CONFIG domain security group of the Unified ICM instance. If there are multiple instances on the server, then the service needs to know which instance security group to authorize against. Therefore, on a multiple Unified ICM instance server, the ICM instance name must be passed as one of the parameters for each request when authorizing a domain user. If an instance name parameter is not passed, then the domain user authorization fails. The local user is free from this requirement because there is only one local group per server. Furthermore, when a domain user is used to access the service, the response is crafted only for the specific instance that user belongs to. However, when a local user tries to access the service, the response includes information for all instances on that server. This gives service providers flexibility to access control information collection for a one or all instances.

On a single instance server, the instance name is not required when you access an API. Because there is only one instance on the server, the domain user is authorized against the CONFIG domain security group of that instance.

The following table summarizes the all authorization combinations. Remember that you can completely disable domain authorization through the service configuration file.

Table 43: Domain Authorization Combination

Unified ICM Instances on Server	User Type	Instance Name Provided	Authorization Criteria	Response Content on Successful Authorization
Multiple	Domain	No	Fail authorization, user must provide instance name in request	HTTP 403 – Access Forbidden
Multiple	Domain	Yes	Authorize against the instance name provided by user	Data for instance requested
Multiple	Local	No	Authorize against local group	Data for all instances
Multiple	Local	Yes	Authorize against local group	Data for instance requested
Single	Domain	No	Automatically detect the instance name and authorize against it	Data for instance installed
Single	Domain	Yes	Authorize against the instance name provided by user. If the instance name is invalid, then authorization fails.	Data for instance installed
Single	Local	No	Authorize against local group	Data for instance installed
Single	Local	Yes	Authorize against local group	Data for instance installed

Encryption

Diagnostic Framework uses SSL to secure the HTTP connection between the server and the client. This secures both the credentials and data exchanged. To establish the SSL connection, the ICM-CCE installer creates a self-signed certificate and uses it during connection negotiation. Because the certificate is self-signed, the browser issues a warning about the invalidity of the certificate trust. Diagnostic Framework allows replacing the self-signed certificate with a trusted third-party certificate. For more information, see the Certificate Management section.

Certificate Management

The ICM-CCE installer creates a self-signed certificate and stores it in the Windows Local Computer Personal certificate store with the friendly name “Cisco ICM Diagnostic Framework service certificate”. The installer then binds this certificate to the Windows HTTP service on the Diagnostic Framework service port, which by default is TCP 7890. The Diagnostic Framework service is hosted on top of the Windows HTTP service. Therefore, this certificate is used by Windows HTTP service to establish a secure HTTPS channel (HTTP over SSL) whenever the Diagnostic Framework service is accessed. The Unified ICM installer uses the Diagnostic Framework Certificate Manager Utility to create and bind the self-signed certificate.

Depending on the nature of business and the network access layout of the site, a self-signed certificate may provide sufficient security for accessing the service from within the trusted intranet. However, if you plan to access the service from outside the trusted network, replace the self-signed certificate with a trusted third-party certificate to provide improved security⁴.

When you access the service with the self signed certificate for the first time from a browser, a warning about the validity of the certificate appears. If you are certain that the server is authentic then you may choose to accept the certificate and store it on the client machine to avoid future warnings.

If you wish to replace the server certificate with a trusted third-party certificate or modify the port to which a certificate is bound, you **must** use the Diagnostic Framework Certificate Manager utility.

Diagnostic Framework Certificate Manager Utility

The Diagnostic Framework Certificate Manager utility is a command line utility used to manage certificate creation and binding for the Diagnostic Framework service. It is installed at `<ICM_Drive>:\icm\serviceability\diagnostics\bin\DiagFwCertMgr.exe`.

The utility can perform the following tasks:

- Create self-signed certificate.
- Store the certificate in Local Computer Personal certificate store.
- Bind a certificate to Windows HTTP service on a given port.
- Remove a certificate binding from the Windows HTTP service on a given port.
- Delete the self-signed certificate created by itself from the Local Computer Personal certificate store.
- Validate the certificate binding to HTTP service for Diagnostic Framework service.

The following section explains the usage of the utility:

```
DiagFwCertMgr /task:<task_name> [/port:<port_number>] [/certhash:<certificate_thumbprint>]
[/logpath:<logfile_path>]
```

⁴ A self-signed certificate cannot guarantee the authenticity of the hosting server. Because the client is unaware of the server authenticity, the client should exercise caution when sharing the user credentials with such server. A malicious user may setup a rogue server with a self-signed certificate, claiming to be a legitimate server, and use it to steal user credentials from the client. Always use trusted certificates to authenticate servers when accessing outside your trusted network.

Where:

- `/task`: specifies the task to be performed.
- `/port`: specifies the port number used by the service; this is optional as the port number is automatically read from the service configuration file (`DiagFwSvc.exe.config`).
- `/certhash`: specifies the SHA-1 thumbprint of the certificate; required only when binding a specific certificate, which exists in the certificate store, to a port.
- `/logpath`: specifies the path where the log file should be created; by default it is the current folder.

The following table explains each task:

Table 44: Diagnostic Framework Certificate Manager Utility Tasks

Task	Description
CreateAndBindCert	Creates a self-signed certificate in the local computer personal certificate store and binds it with HTTP service on the given port. (Used by ICM-CCEInstall)
BindCertFromStore	Looks up the certificate provided by <code>/certhash</code> argument in certificate store and binds it with the HTTP service on the given port.
UnbindCert	Removes the certificate binding from the specified port, does not modify any certificate in the store.
UnbindAndDeleteCert	Removes the certificate binding from the specified port. Also, deletes the self-signed certificate created by <code>CreateAndBindCert</code> option. (Used by ICM-CCE Uninstall)
ValidateCertBinding	Verifies the certificate binding on the specified port and confirms its presence in the local computer certificate store.
CreateAndAddToStoreCertECDSA	Creates and stores the self-signed ECDSA certificate in the local computer certificate store without binding it to the port.
CheckAndCreateStoreCertECDSA	Checks if the certificate is present in the store and creates only if it is NOT present.
CreateAndBindCertECDSA	Creates a self-signed ECDSA certificate in the local computer certificate store and binds it with HTTP service on the given port.
DeleteCertECDSA	Deletes the self-signed ECDSA certificate.
UnbindAndDeleteCertECDSA	Removes the certificate binding from the specified port. Also, deletes the self-signed ECDSA certificate created by CreateAndBindCertECDS option.

Diagnostic Framework Certificate Manager utility stores the thumbprint (SHA-1 hash) of the self-signed certificate created by the utility and the certificate used by the Diagnostic Framework service in the registry at the following location respectively:

```
HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\Serviceability\
DiagnosticFramework\SelfSignedCertCreatedForDiagFwSvc
HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\Serviceability\
DiagnosticFramework\CertUsedByDiagFwSvc
```

Unless the certificate used by the service is changed manually, both registry values are the same.

Using a Trusted Third-Party Certificate

Replacing the certificate used by the Diagnostic Framework service involves two tasks. The first task is to import the new certificate in the Local Computer Personal certificate store. The second task is to bind it with the TCP port used by the service.

Import Certificate

Select **Run** from the **Start** menu, and then enter `mmc`. MMC appears.

From the **File** menu, select **Add/Remove Snap In**. The **Add or Remove Snap-ins** appears.

Use the MMC Certificates snap-in to import a certificate in the Local Computer Personal certificate store. See Microsoft documentation for details on Importing the Certificate into the Local Computer Store.



Caution Diagnostic Framework does not use IIS web server. It is hosted on top of Windows HTTP service. Use the DiagFwCertMgr utility to bind this certificate to the Windows HTTP service.

Bind Certificate

Complete the following instructions to bind the certificate added to the Windows HTTP service using the DiagFwCertMgr utility:

1. Open MMC Certificates snap-in and record the thumbprint of the certificate to use with the Diagnostic Framework service.
2. Stop the Diagnostic Framework service via the Windows service control.
3. Open a command prompt and change directory to
`<ICM_Drive>:\icm\serviceability\diagnostics\bin.`
4. In the command window, run the command **DiagFwCertMgr /task:UnbindCert** to remove the current certificate binding from the port.
5. Run the command **DiagFwCertMgr /task:BindCertFromStore /certhash:<hash of the certificate noted above>** to bind the new certificate to the service.

The utility reads the port number from the service configuration file.

6. Read the output and confirm that the preceding command completed successfully.
7. Optionally, run the `DiagFwCertMgr /task:ValidateCertBinding` command to verify the changes to the certificate binding.
8. Restart the Diagnostic Framework service.

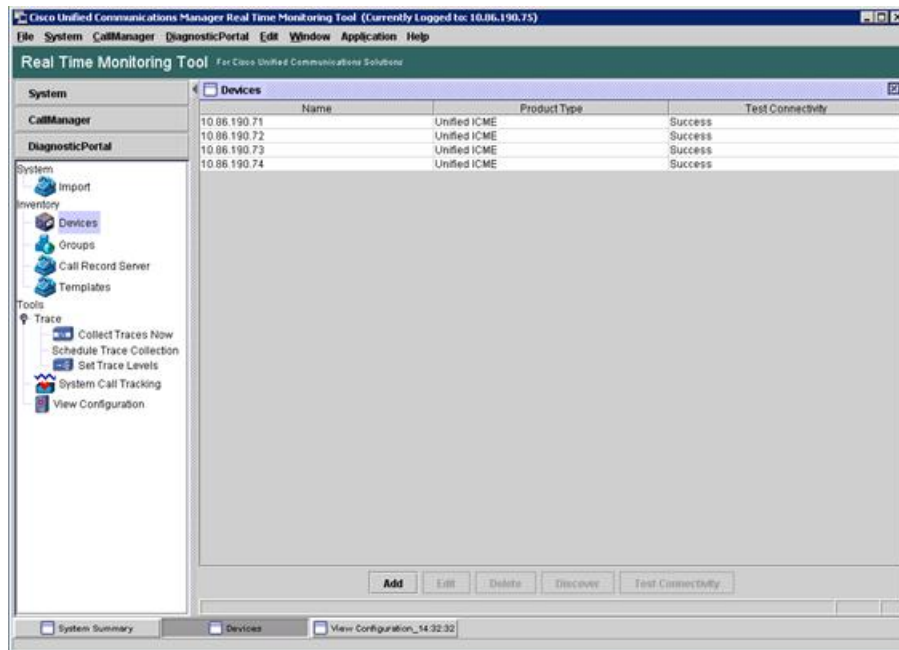
Usage

The framework provides four ways to access the diagnostic data:

Accessing the Diagnostic Framework Through the Analysis Manager

The Analysis Manager is part of the Real Time Monitoring client Tool (RTMT) that resides on Unified CM. RTMT is not a web-based tool, rather it is a thick client tool that you must download from the Unified CM and install on a server. RTMT includes menus for the Analysis Manager. You can access the Analysis Manager functions from the tool. See the sample screen:

Figure 27: Real Time Monitoring Tool



For more information about how to use the Analysis Manager, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>.

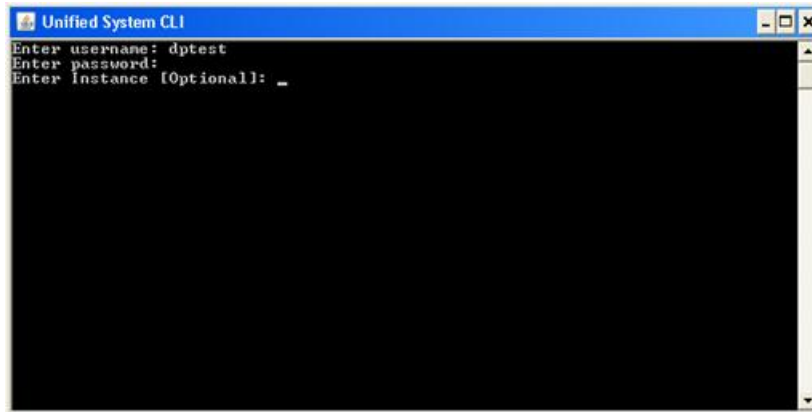
Accessing the Diagnostic Framework Through the Unified System CLI

You can also access the Diagnostic Framework through a CLI. The CLI access utility is installed on every Unified ICM machine at `<ICM_Drive>:\icm\serviceability\wsccli\runwsccli.bat`.

Use a DOS command shell to run this batch file, and it sets up everything needed to access the Diagnostic Framework through the CLI.

A shortcut is included to the Unified ICM menu to provide quick access to the CLI. Also, you can access Unified CLI from **Start > Programs > Cisco Unified ICM-CCE Tools > Unified CLI**. A new DOS Window opens with an initial prompt for your credentials (username and password).

Figure 28: Using Unified System CLI from Command Prompt



On authentication, you can use the CLI from this window, as explained in [Unified CLI Architecture](#), on page 163.

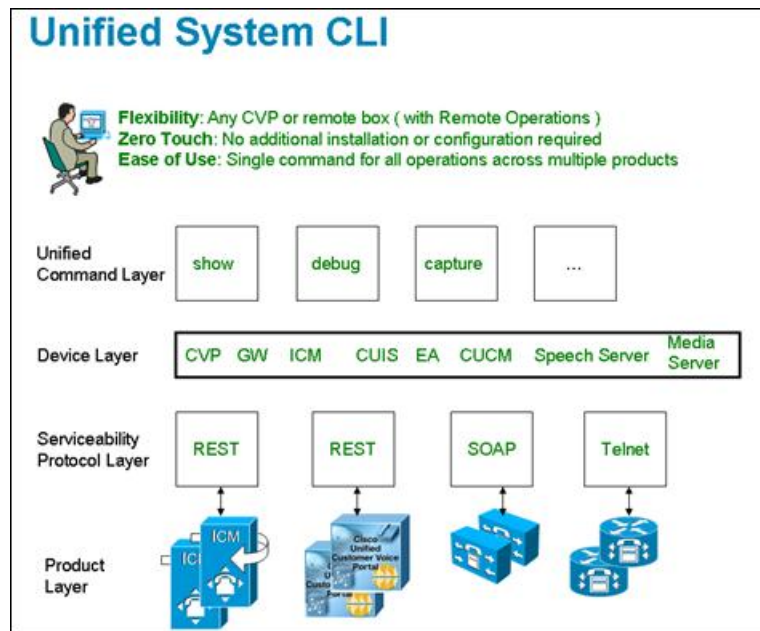
The CLI allows an optional user input named Instance. In Unified CCE environments, you do not enter anything. In a Hosted environment, you must enter the instance to access the diagnostic data for only that particular instance. For more information, see [Special Consideration for Servers with Multiple Unified ICM Instances](#), on page 158.

Unified CLI Architecture



Note This figure is only from a Unified CVP perspective, and does not directly specify the Diagnostic Framework. However, the Diagnostic Framework is what the Unified CCE uses as an underlying implementation.

Figure 29: Unified CLI Architecture



A user can perform the following tasks using the Unified CLI:

- Run a single command (in system mode) on any Unified CCE system to gather information about all supported solution components.
- In system mode, you can optionally provide the seed devices in WSC_CLI_DIR\conf directory or give a flat CSV file with a device list.
- System mode allows the CLI to recursively go to each supported box in the background and run the same command that the user ran in system mode. User can optionally limit the system command to be run only on certain device group or list of servers. Device group is automatically populated based on device type (Unified CVP, Unified ICM, Cisco IOS Firewall, EA as an example), device IP/hostname wildcard (LOC-1*, 10.86.129.* as an example for branch office deployments), or the CSV file in WSC_CLI_DIR\conf directory.
- You can run the system command by prefixing the “system” on any regular command. For example, “system show all” or typing “system” and running the commands exactly like a regular CLI for interactive mode.

Unified System CLI Usability

- System CLI is automatically installed on all Unified CCE systems as part of the infrastructure, so there is no additional installation required.
- System CLI can be run as a Windows scheduled job or a Unix Cron job. Single command for all operations across multiple products and servers.
- All the commands available in non-system mode for a local system are available in system mode. The command syntax remains the same in system mode. There is an additional option to limit the system command option to certain device group, device type or list of servers.
- In system mode, when you seek help for using the “?” character after you enter the keyword component or subcomponent, the list of components that appears maybe large due to the fact that it is an aggregated list of all the possible component types on all the unique server types.
- The primary list is defined by the unique “Name,” “ProductType.” If there are multiple components for the purpose of co-location, the internal list contains one entry because there is only one WebServices manager running at the specified port.
- System CLI runs on a low priority, so it only uses the IDLE CPU on the System. It should not affect the Call Processing even if it runs on a system working under load. The response time varies depending on the load of the system you are running and the server response time. The response time when there is no running load should be below 5 seconds for each server for simple operations like “version,” “license,” “debug” and “perf.” The response time when there is no running load for “platform” should be below 10 seconds for each server. However, the response time cannot be determined for commands like “trace,” “log,” “sessions,” and all “tech-support” that can vary depending on the data transferred by the server.
- There are no specific timeouts on the System CLI client and it is controlled by the server.
- Error code and error description during failure conditions occur from the server side. System CLI displays the error message arriving from server. The possible error codes are specified and described in the DP REST API specification.

Extensibility

System CLI is not a tool but an extensible platform to build several analysis toolkits. The CLI library can be embedded or used within the analysis engine to do post processing of the data (normalized). System CLI can be used by common scripting tools like Perl to create custom logic.

Command Syntax

The common CLI syntax matches closely with Cisco IOS gateway CLI commands. In cases where specific commands or parameters are not available in IOS gateway, the syntax attempts to match the Unified CM platform CLI commands for consistency.

The following tables list and describe the CLI commands that are available for diagnostic purposes.

Note If you do not specify component/sub-component, then the list includes all the installed components/sub-components on the server.

The command output on screen does not include binary data.

Table 45: CLI Commands

Command (Verb)	Noun	Description
show	all	Aggregation of output for all the supported nouns and specific to the verb “show.”
	component	Lists the currently installed components on the server.
	configuration	Lists the application configuration.
	debug	Shows the current debug levels.
	license	Shows the license/port information.
	log	Shows the logs.
	perf	Shows the performance information.
	platform	Shows the platform information.
	sessions	Shows the current active sessions/calls. (Not supported by Unified CCE)
	tech-support	Shows system information for Tech-Support. Note This command is exactly the same as “show all”.
	trace	Shows the traces.
	version	Shows system hardware and software status and version.
devices	Shows information of devices that are known to the CLI.	
debug	level	Sets the specific debug level.
help	—	Shows the help information.
quit	—	Quits the CLI.
capture	—	Captures the network packets. (Not supported by Unified CCE)



Note You can enter the start of a command and press **Tab** to complete the command. For example, if you enter **show all comp** and press **Tab**, **show all component** is completed.

You can enter a full command name and press **Tab** to display all the commands or subcommands that are available. For example, if you enter **show** and press **Tab**, you see all the **show** subcommands.

Detailed help that includes a definition of each command and examples of usage is available in the online help.

To get detailed help, at the CLI prompt, enter **help <command>** where *command* specifies the command name or the command and parameter.

To query only command syntax, at the CLI prompt, enter **<command> ?** where *command* represents the command name or the command and parameter.



Note The filter and match features of the CLI are not supported for trace files because the framework returns a zip file that contains not just the text file. For those two features, CLI expects a plain text file.

show all

Syntax

```
show all [options]
```

This command provides information for the component or subcomponent based on the command filters.

Options

component

narrow the output to the specified component(s). The option is limited to trace, debug, perf and sessions commands.

subcomponent

narrow the output to the specified subcomponent(s). The option is limited to trace, debug, perf and sessions commands.

absdatetime

narrow the output to the specified time range in the form of start time and end time. Time format is “mm-dd-yyyy:hh:mm”.

brief

This option is used to prevent the command from collecting certain default logs.



Note This command is used only in Unified CCE to avoid collecting OPC and VRU capture files by default.

retime

narrow the output to the specified time range in the form of relative time from the current time.

match

narrow the output to the specified regex pattern. This match pattern is applied to text based log output only. The option is limited to trace and log commands.

filter

narrow the output to the specified command(s).

redirect

redirect the output to a file or a directory.

Additional System Mode Options**devicetype**

narrow the output to the specified device type(s).

server

narrow the output to the specified device(s).

sysmatch

narrow the output to the list of servers matched with a regexp for hostnames or ip addresses.

group

narrow the output to the specified group name(s).

dtcomponent

narrow the output to the specified component(s) for a device type of the specified component.

dtsubcomponent

narrow the output to the specified subcomponent(s) for a device type of the specified subcomponent.

Examples

```
show all component cvp:CallServer
```

```
show all component cvp:CallServer subcomponent cvp:SIP
```

```
show all component cvp:CallServer|cvp:VoiceXMLServer subcomponent cvp:SIP|cvp:VXMLServer
```

```
show all component cvp:CallServer subcomponent cvp:SIP filter race|log|version
```

```
show all retime 2 hours
```

In System Mode

```
show all devicetype ios
```

```
show all devicetype ios|cvp
```

```
show all server 10.86.129.11(cvp)
```

```
show all group GroupA|default
```

show all dtcomponent "ucm:Cisco CallManager|cup:Cisco UP SIP Proxy" -- Extract everything from all devices except ucm and cup where device specific filters are applied.

By default, the output zip file is saved at WSC_CLI_DIR\download directory where WSC_CLI_DIR is the environment variable.

To save the output to a specific directory, show all redirect dir c:\temp\ -- the output is saved in c:\temp\clioutput.zip.

To save the output to a text file, show all redirect file c:\temp\output.txt

show tech-support

Syntax

```
show tech-support [options]
```

This command provides information for the component or subcomponent based on the command filters similar to the "show all" command.

Options

brief

This option is used to prevent the **show tech-support** command from collecting certain default logs.



Note This command is used only in Unified CCE to avoid collecting OPC and VRU capture files by default.

Example

show tech-support brief

In Unified CCE, this command downloads logs for all components excluding OPC and VRU capture files. In other products, this command behaves the way "show tech-support" command does.

```
show tech-support brief absdatetime 9-18-2008:14:00 9-20-2008:18:00 redirect C:\temp\
```

In Unified CCE, this command downloads logs for all components excluding OPC and VRU capture files for the specified start and end time. In other products, this command behaves the way "show tech-support" command does. The output is saved in c:\temp\clioutput.zip.

```
show tech-support component "icm:Peripheral Gateway 1A" subcomponent "icm:opc" absdatetime 9-18-2008:14:00 9-20-2008:18:00 brief redirect C:\temp\
```

In Unified CCE, this command downloads logs for the component Peripheral Gateway 1A and subcomponent OPC for the specified date and time. The output is saved in C:\temp\clioutput.zip. Removing **brief** from the command results in collection of OPC captures as well.

show component

Syntax

```
show component [options]
```

Lists all the installed subcomponents of a component. If component is not given, then all the components and subcomponents configured/installed are listed.

Options

Name of a specific component.

Example

```
show component cvp:VXMLServer
```

show config

Syntax

```
show config [options]
```

This command displays the configuration data.

Options**component**

narrow the output to the specified component(s).

subcomponent

narrow the output to the specified subcomponent(s).

redirect

redirect the output to a file or a directory.

Additional System Options**devicetype**

narrow the output to the specified device type(s).

server

narrow the output to the specified device(s).

sysmatch

narrow the output to the list of servers matched with a regexp for host names or IP addresses.

group

narrow the output to the specified group name(s).

Example

```
show config component cvp:CallServer subcomponent cvp:H323
```

In System Mode

```
show config devicetype ios
```

```
show config devicetype ios|cvp
```

```
show config server 10.86.129.11(cvp)
```

```
show config group CVPAndIOS|default
```

To save the output to a directory, show config redirect dir c:\temp\ -- the output is saved in c:\temp\clioutput.zip.

To save the output to a text file, show config redirect file c:\temp\output.txt

show debug

Syntax

```
show debug [options]
```

This request returns the current debug level for a component or subcomponent.

Options**component**

narrow the output to the specified component(s).

subcomponent

narrow the output to the specified subcomponent(s).

redirect

redirect the output to a file or a directory.

Additional System Options**devicetype**

narrow the output to the specified device type(s).

server

narrow the output to the specified device(s).

sysmatch

narrow the output to the list of servers matched with a regexp for host names or IP addresses.

group

narrow the output to the specified group name(s).

dtcomponent

narrow the output to the specified component(s) for a device type of the specified component.

dtsubcomponent

narrow the output to the specified subcomponent(s) for a device type of the specified subcomponent.

Valid Debug Levels

level 0

Default debug level. During general operation, product log errors or warning trace messages.

level 1

Small performance impact (Warning) debug level. Can be run on production environment. At level 1, additional basic component traces along with level 0 trace messages.

level 2

Medium performance impact (Informational) debug level. Can be run on production environment. At level 2, additional detailed component traces along with level 1 trace messages.

level 3

High performance impact (Debug) debug level. Can be run on production environment. At level 3, most detailed trace messages will be logged along with level 2 trace messages.

level 4

Cannot be run on production environment. At level 4, internal subcomponent trace messages will be logged along with level 3 trace messages.

level 5

Cannot be run on production environment. At level 5, internal functional module trace messages will be logged along with level 4 trace messages.

level 99

Custom debug level. In the case when log levels do not match, 99 will be returned as custom level along data representing the custom debug settings.

Example

```
show debug component cvp:CallServer
```

```
show debug component cvp:CallServer|cvp:VXMLServer subcomponent cvp:H323|cvp:SIP
```

In System Mode

```
show debug devicetype cup|ucm|icm
```

```
show debug devicetype ios|cvp
```

```
show debug server 10.86.129.11(cvp)|10.86.129.123(ucm)
```

```
show debug group GroupB|default
```

```
show debug dtcomponent "ucm:Cisco CallManager|cup:Cisco UP SIP Proxy|cvp:CallServer"
```

To save the output to a directory, show debug redirect dir c:\temp\ -- the output is saved in c:\temp\clioutput.zip.

To save the output to a text file, show debug redirect file c:\temp\output.txt

*show license***Syntax**

```
show license [options]
```

This command displays the license data.

Options**redirect**

redirect the output to a file or a directory.

Additional System Options**devicetype**

narrow the output to the specified device type(s).

server

narrow the output to the specified device(s).

sysmatch

narrow the output to the list of servers matched with a regexp for hostnames or ip addresses.

group

narrow the output to the specified group name(s).

Example

```
show license
```

In System Mode

```
show license devicetype ios|cvp|ucm
```

```
show license server 10.86.129.123(ucm)
```

```
show license group GroupB|default
```

To save the output to a directory, show license redirect dir c:\temp\ -- the output is saved in c:\temp\clioutput.zip.

To save the output to a text file, show license redirect file c:\temp\output.txt

*show log***Syntax**

```
show log [options]
```

Displays contents or downloads (if redirect option is used) the product *miscellaneous* log file(s) for a component or subcomponent.

Options**component**

narrow the output to the specified component(s).

subcomponent

narrow the output to the specified subcomponent(s).

absdatetime

narrow the output to the specified time range in the form of start time and end time. Time format is “mm-dd-yyyy:hh:mm”.

reltime

narrow the output to the specified time range in the form of relative time from the current time.

match

narrow the output to the specified regex pattern. This match pattern is applied to text based log output only.

redirect

redirect the output to a file or a directory.

Additional System Options**devicetype**

narrow the output to the specified device type(s).

server

narrow the output to the specified device(s).

sysmatch

narrow the output to the list of servers matched with a regexp for hostnames or ip addresses.

group

narrow the output to the specified group name(s).

Example

show log component cvp:callserver - displays contents of all the log files for component cvp:callserver; can be a huge output

show log component cvp:vxmlserver absdatetime 9-18-2008:14:00 9-20-2008:18:00 - displays contents of all the log files for component cvp:vxmlserver based on specific start date,time and end date, time values

show log component cvp:vxmlserver absdatetime 9-18-2008:14:00 13:00 - displays contents of all the log files for component cvp:vxmlserver based on specific start date,time and end time values.

show log component cvp:callserver subcomponent sip reltime 10 minutes – displays contents of all the log files based on elapsed time of 10 minutes for component cvp:callserver and subcomponent cvp:sip

show log component cvp:callserver absdatetime 9-18-2008:14:00 13:00 match .*CVPServlet.* - displays contents of all the log files based on match criteria, time range for component cvp:callserver

show log component cvp:callserver absdatetime 9-18-2008:14:00 13:00 match .*CVPServlet.* redirect file c:\ucceLogs - downloads all the log files on match criteria, time range for component cvp:callserver

To save the output to a directory, show log redirect dir c:\temp\ -- the output is saved in c:\temp\clioutput.zip.

To save the output to a text file, show log redirect file c:\temp\output.txt

show perf

Syntax

```
show perf [options]
```

This command displays performance data.

Options

component

narrow the output to the specified component(s).

subcomponent

narrow the output to the specified subcomponent(s).

redirect

redirect the output to a file or a directory.

Additional System Options

devicetype

narrow the output to the specified device type(s).

server

narrow the output to the specified device(s).

sysmatch

narrow the output to the list of servers matched with a regexp for hostnames or ip addresses.

group

narrow the output to the specified group name(s).

dtcomponent

narrow the output to the specified component(s) for a device type of the specified component.

dtsubcomponent

narrow the output to the specified subcomponent(s) for a device type of the specified subcomponent.

Example

```
show perf component cvp:CallServer subcomponent cvp:ICM
```

In System Mode

```
show perf devicetype ios|cvp
```

```
show perf server 10.86.129.11(cvp)
```

```
show perf group GroupB|default
```

To save the output to a directory, show perf redirect dir c:\temp\ -- the output is saved in c:\temp\clioutput.zip.

To save the output to a text file, show perf redirect file c:\temp\output.txt

show platform

Syntax

```
show platform [options]
```

Shows information about the operating system and hardware.

Options**redirect**

redirect the output to a file or a directory.

Additional System Options**devicetype**

narrow the output to the specified device type(s).

server

narrow the output to the specified device(s).

sysmatch

narrow the output to the list of servers matched with a regexp for hostnames or ip addresses.

group

narrow the output to the specified group name(s).

Example

```
show platform
```

In System Mode

```
show platform devicetype ios|cvp|ucm
```

```
show platform server 10.86.129.11(cvp)
```

```
show platform group GroupB|default
```

To save the output to a directory, show platform redirect dir c:\temp\ -- the output is saved in c:\temp\clioutput.zip.

To save the output to a text file, show platform redirect file c:\temp\output.txt

show sessions

Syntax

```
show sessions [options]
```

This request returns active session status/information.

Options

component

narrow the output to the specified component(s).

subcomponent

narrow the output to the specified subcomponent(s).

redirect

redirect the output to a file or a directory.

Additional System Options

devicetype

narrow the output to the specified device type(s).

server

narrow the output to the specified device(s).

sysmatch

narrow the output to the list of servers matched with a regexp for hostnames or ip addresses.

group

narrow the output to the specified group name(s).

Example

```
show sessions component cvp:CallServer subcomponent cvp:IVR
```

To save the output to a directory, show sessions redirect dir c:\temp\ -- the output is saved in c:\temp\clioutput.zip.

To save the output to a text file, show sessions redirect file c:\temp\output.txt

*show trace***Syntax**

```
show trace [options]
```

Displays contents or downloads (if redirect option is used) the product trace file(s) for a component or subcomponent.

Options**component**

narrow the output to the specified component(s).

subcomponent

narrow the output to the specified subcomponent(s).

absdatetime

narrow the output to the specified time range in the form of start time and end time. Time format is “mm-dd-yyyy:hh:mm”.

reltime

narrow the output to the specified time range in the form of relative time from the current time.

match

narrow the output to the specified regex pattern. This match pattern is applied to text based log output only.

redirect

redirect the output to a file or a directory.

Additional System Options**devicetype**

narrow the output to the specified device type(s).

server

narrow the output to the specified device(s).

sysmatch

narrow the output to the list of servers matched with a regexp for hostnames or ip addresses.

Group

narrow the output to the specified group name(s).

dtcomponent

narrow the output to the specified component(s) for a device type of the specified component.

dtsubcomponent

narrow the output to the specified subcomponent(s) for a device type of the specified subcomponent.

Example

show trace component cvp:callserver - displays contents of all the trace files for component cvp:callserver, can be a huge output

show trace component cvp:vxmlserver absdatetime 9-18-2008:14:00 9-20-2008:18:00 - displays contents of all the trace files for component cvp:vxmlserver based on specific start date,time and end date, time values

show trace component cvp:vxmlserver absdatetime 9-18-2008:14:00 13:00 – displays contents of all the trace files for component cvp:vxmlserver based on specific start date,time and end time values.

show trace component cvp:callserver subcomponent cvp:sip reltime 10 minutes - displays contents of all the trace files based on elapsed time of 10 minutes for component cvp:callserver and subcomponent cvp:sip

show trace component cvp:callserver absdatetime 9-18-2008:14:00 13:00 match .*CVP_7_0_SIP-7.* - displays contents of all the trace files based on match criteria, time range for component cvp:callserver

show trace component cvp:callserver absdatetime 9-18-2008:14:00 13:00 match .*CVP_7_0_SIP-7.* redirect c:\uccelogs - downloads all the trace files on match criteria, time range for component cvp:callserver

To save the output to a directory, show trace redirect dir c:\temp\ -- the output is saved in c:\temp\clioutput.zip.

To save the output to a text file, show trace redirect file c:\temp\output.txt

show version

Syntax

```
show version [options]
```

Shows product software version.

Options**redirect**

redirect the output to a file or a directory.

Additional System Options**devicetype**

narrow the output to the specified device type(s).

server

narrow the output to the specified device(s).

sysmatch

narrow the output to the list of servers matched with a regexp for hostnames or ip addresses.

group

narrow the output to the specified group name(s).

Example

```
show version
```

In System Mode

```
show version devicetype ios|cyp|ucm
```

```
show version server 10.86.129.11(cyp)
```

```
show version group GroupB|default
```

To save the output to a directory, show version redirect dir c:\temp\ -- the output is saved in c:\temp\clioutput.zip.

To save the output to a text file, show version redirect file c:\temp\output.txt

show devices

Syntax

```
show devices [options]
```

List device information including hostname/ip address and port numbers.

Options**redirect**

redirect the output to a file or a directory.

Additional System Options**devicetype**

narrow the output to the specified device type(s).

server

narrow the output to the specified device(s).

sysmatch

narrow the output to the list of servers matched with a regexp for hostnames or ip addresses.

group

narrow the output to the specified group name(s).

Example

```
show devices
```

To save the output to a directory, show devices redirect `dir c:\temp\ --` the output is saved in `c:\temp\clioutput.zip`.

To save the output to a text file, show devices redirect file `c:\temp\output.txt`

debug level

Syntax

```
debug level levelnumber [options]
```

This command is used to set debug level. Valid levels range from integer values between 0 - 5.

Options

component

narrow the output to the specified component(s).

subcomponent

narrow the output to the specified subcomponent(s).

redirect

redirect the output to a file or a directory.

Additional System Options

devicetype

narrow the output to the specified device type(s).

server

narrow the output to the specified device(s).

sysmatch

narrow the output to the list of servers matched with a regexp for hostnames or ip addresses.

group

narrow the output to the specified group name(s).

dtcomponent

narrow the output to the specified component(s) for a device type of the specified component.

dtsubcomponent

narrow the output to the specified subcomponent(s) for a device type of the specified subcomponent.

Debug Levels

level 0

Default debug level. During general operation, product log errors, or warning trace messages.

level 1

Small performance impact (Warning) debug level. Can be run on production environment. At level 1, additional basic component traces along with level 0 trace messages.

level 2

Medium performance impact (Informational) debug level. Can be run on production environment. At level 2, additional detailed component traces along with level 1 trace messages.

level 3

High performance impact (Debug) debug level. Can be run on production environment. At level 3, most detailed trace messages will be logged along with level 2 trace messages.

level 4

Cannot be run on production environment. At level 4, internal subcomponent trace messages will be logged along with level 3 trace messages.

level 5

Cannot be run on production environment. At level 5, internal functional module trace messages will be logged along with level 4 trace messages.

level 99

Custom debug level. In the case when log levels do not match, 99 will be returned as custom level along data representing the custom debug settings.

Example

```
debug level 1 component cvp:CallServer
```

```
debug level 2
```

```
debug level 99 custom app-defined-data component cvp:callserver subcomponent cvp:sip
```

In System Mode

```
debug level 0 devicetype cup|ucm|icm
```

```
debug level 1 devicetype ios|cvp
```

```
debug level 2 server 10.86.129.11(cvp)|10.86.129.123(ucm)
```

```
debug level 3 group GroupB|default
```

```
debug level 3 dtcomponent "ucm:Cisco CallManager|cup:Cisco UP SIP Proxy|cvp:CallServer"
```

To save the output to a directory, debug level 1 redirect dir c:\temp\ -- the output is saved in c:\temp\clioutput.zip.

To save the output to a text file, debug level 1 redirect file c:\temp\output.txt

System Mode Syntax

Following is the system mode syntax.

Note You can add product specific extensions; however, any extension must be reviewed by this common cross-product team for clarity and consistency.

Table 46: System Mode Syntax

Command (Verb)	Noun	Description
system		Enter the interactive system mode of the CLI. Use quit/exit command to exit the system mode.

System Command (show all)

Syntax

show all

The system command can also be run by prefixing the “system” on any regular command for non-interactive mode. For example, “system show all”.

Parameters

[component *component(s)*] [subcomponent *subcomponent(s)*] [filter *noun(s)*] [absdatetime *startdate* *enddate*] [reltime <value> minutes/hours/days/weeks/months] [match <string value>] [*<output modifier>*] [**group** *group(s)*] [**server** *server(s)*][**sysmatch** <string value>][**devicetype** <product type>]



Note The options highlighted in bold above are included to commands in system mode.

Options

group

narrows the output to selected group(s) only.

server

narrows the output to selected server(s) only.

sysmatch

match a particular string as specified by <string value>.



Note The command notifies about a possible impact to system performance and asks you if you want to continue.



Warning Because running this command can affect system performance, run the command during off-peak hours.

Aggregation of output for all the supported nouns and specific to the verb “show”.

Example-1

```
admin:system
admin(system):show all redirect dir c:\system-tech-support
[server-1]
  server-1 show all Output
[server-2]
  server-2 show all Output
[server-3]
  server-3 show all Output
[server-4]
  server-4 show all Output
[server-5]
  server-5 show all Output
[server-6]
  server-6 show all Output
```

Output is saved to "c:\system-tech-support\clioutput0.zip"

Example-2

Assuming Group:Branch-1 contains server-2, server-3 and Group:Branch-2 contains server-5, server-6

```
admin:system
admin(system): show all group Branch1 | Branch2 redirect dir c:\system-tech-support
[server-2]
  server-2 show all Output
[server-3]
  server-3 show all Output
[server-5]
  server-5 show all Output
[server-6]
  server-6 show all Output
```

Output is saved to "c:\system-tech-support\clioutput0.zip"

Example-3

```
admin:system
admin(system):show all server server-1 | server-6 redirect dir c:\system-tech-support
[server-1]
  server-1 show all Output
[server-6]
  server-6 show all Output
```

Output is saved to "c:\system-tech-support\clioutput0.zip"

Example-4

Assuming that server-2, server-3, server-5 are in subnet 10.86.129.xxx

```
admin:system
admin(system):show all group Branch1 | Branch2 sysmatch redirect dir c:\system-tech-support

[server-2]
  server-2 show all Output
[server-3]
  server-3 show all Output
```

```
[server-5]
server-5 show all Output

Output is saved to "c:\system-tech-support\clioutput0.zip"
```

Example-5

```
admin:system show all redirect ftp://vpalawat:password/SR609140000
[server-1]
server-1 show all Output
[server-2]
server-2 show all Output
[server-3]
server-3 show all Output
[server-4]
server-4 show all Output
[server-5]
server-5 show all Output
[server-6]
server-6 show all Output

Output is saved to "ftp-sj.cisco.com\incoming\SR609140000-0.zip"
Output is saved to "ftp-sj.cisco.com\incoming\SR609140000-1.zip"
```

Example-6

Assuming that devices configured in OAMP are CVP[server-5], IOS [server-2, server-3], UCM [server-4] and ICM [server-1] .

```
admin:system
admin(system):show all devicetype cvp|ios redirect dir c:\system-tech-support
[server-2]
server-2 show all Output of ProductType [ios]
[server-3]
server-3 show all Output of ProductType [ios]
[server-5]
server-5 show all Output of ProductType [cvp]

Output is saved to "c:\system-tech-support\clioutput0.zip"
```

Run Automated Commands

CLI or System CLI commands can be run automatically using the following mechanism:

- Create a batch file with the commands given below as an example:

```
REM VERSION-COLLECTION
echo system show version redirect dir c:\test\ > clicmds.txt
echo exit >> clicmds.txt
type clicmds.txt | wsccli.bat inplace nointeractive "user:wsmadmin" "passwd:<password>"
```

- To define a multiple component and sub-component filter, use double quotes as follows:

```
REM CONFIG-COLLECTION
echo show config comp CallServer subc "SIP|ICM" redirect dir c:\test\ > clicmds.txt
echo exit >> clicmds.txt
type clicmds.txt | wsccli.bat inplace nointeractive "user:wsmadmin" "passwd:<password>"
```

- Automated trace collection on CVP servers using a scheduled job:

```

REM TRACE-COLLECTION
echo show trace device cvp redirect dir c:\test\ > clicmds.txt
echo exit >> clicmds.txt
type clicmds.txt | wsccli.bat inplace nointeractive "user:wsmadmin" "passwd:<password>"

```

- Automated script can be invoked from a Windows scheduled job for automated tasks.



Note Note: Because running the automated commands and non-interactive mode can affect system performance, run the command during off-peak hours.

Import File Syntax

The file to be imported is <ICM_Drive>:\icm\serviceability\wsccli\conf\devices.csv.

A sample file named devices-sample.csv is provided. Add the devices to this file, and then restart the Unified System CLI to load those devices.

Devices CSV File Syntax

```

#####
# Sample CSV file for importing devices. File name should be devices.csv
# The file should be in the WSC_CLI_DIR/conf folder
#
# The possible values for Product Type are given below:
#
# * UCM - For Unified CM
# * CVP - For Unified CVP
# * ICM - For Unified ICME, Unified ICM
# * UCCX- For Unified CCX
# * IOS - For IOS Gateway
# * EA - For Unified Expert Advisor
# * CUIC - For Unified Intelligence Center
# * CUP - For Unified Presence ( that includes the SIP Proxy )
#####
#
# The column assignments are as follows:
#
# HOSTNAME -- Mandatory
# DESCRIPTION
# PRODUCT_TYPE -- Mandatory
# GROUP
# USERNAME
# PASSWORD
# PORT_NUMBER -- Mandatory
# ENABLE_PASSWORD
# IS_SEED_SERVER
#
HOSTNAME, DESCRIPTION, PRODUCT_TYPE, GROUP, USERNAME, PASSWORD, PORT_NUMBER,
ENABLE_PASSWORD,
IS_SEED_SERVER #10.86.129.109, IOS GW, IOS, Location_1, cisco, cisco, 22, cisco,

```



Note All references to ICM in the above text file equal Unified CCE.

Device, Protocol and Command Mapping Table

The mapping table for device type, command, and serviceability protocol created in WSC_CLI_DIR/conf folder is as follows:

Table 47: Device, Protocol, and Command Mapping

	CVP	Unified CCE	EA	CUIC / LiveData	Speech Server	Media Server	Trace Server	IOS GW	Unified CM	Unified CCX	Finesse
capture	REST	✘	✘	✘	REST	REST	REST	✘	✘	✘	✘
config	REST	REST	REST	✘	✘	✘	✘	TELNET/SSH	✘	✘	✘
debug	REST	REST	REST	✘	✘	✘	✘	TELNET/SSH	SOAP	REST	✘
license	REST	REST	REST	✘	?	✘	✘	TELNET/SSH	SOAP	REST	✘
log	REST	REST	✘	✘	REST	REST	REST	✘	✘	✘	✘
perf	REST	REST	✘	✘	REST	REST	REST	TELNET/SSH	✘	✘	✘
platform	REST	REST	SOAP	SOAP	REST	REST	REST	TELNET/SSH	SOAP	SOAP	SOAP
sessions	REST	✘	✘	✘	✘	✘	✘	TELNET/SSH	✘	✘	✘
trace	REST	REST	SOAP REST	SOAP REST	?	?	?	TELNET/SSH	SOAP	SOAP REST	SOAP
version	REST	REST	SOAP REST	SOAP REST	REST	REST	REST	TELNET/SSH	SOAP	SOAP REST	SOAP

✘ — Not supported ? — Actual



Note Cisco Finesse does not support System CLI for system trace settings.



Note By default from the release 12.5(2) onwards, for IOS GW in the sample devices CSV file the port number is 22. When you want to use Telnet modify the port number to 23.

CLI has the primary list of all devices from seed servers. It runs the system command on each device recursively based on the protocol supported in this release and according to the mapping table given above.

Primary list is defined by the unique “Name”, “ProductType”. If there are multiple devices for the purpose of co-location, the internal list still contains one entry for a product type because there is only one WebServices manager running at the specified port.

CLI also pulls the component/sub-component list from all the devices to create a primary list dynamically.

The CLI output is in the structure of **[Server] / [Type] / clioutput**. A single (or multiple zip in case exceeding the size of zip file of 1GB) zip file is created for the aggregate response from all servers.

Mapping of System CLI Commands to IOS CLI Commands

Note This mapping table is available in the configuration file, so that mapping can be easily altered.

Table 48: Mapping of System CLI Commands to IOS CLI Commands

System CLI	IOS CLI
“show config”	“show running-config”
“show version”	“show version”
“show license”	“show license”
“show perf”	“show call resource voice stat” “show memory statistics” “show processes cpu history” “show processes memory sorted” “show voice dsp group all” “show voice dsp voice”
“show debug”	“show debug”
“show log”	N/A
“show sessions”	“show call active voice compact”
“show tech-support”	“show tech-support” <Everything else given above>
“show trace”	“show logging”
“show platform”	“show diag”
“debug”	<pre> 0 no debug all 1 - deb ccsip err deb cch323 err deb voip app vxml err deb http client err deb mrcp err deb rtsp err deb h225 asnl err deb h245 asnl err 2 - debug isdn q931 debug h225 events debug h245 events debug voip ccapi inout debug vtsp events 3 - debug ccsip messages debug h225 q931 debug h225 asnl debug h245 asnl </pre>

Logs

You can find all logs generated by the CLI process under the directory
<ICM_Drive>:\icm\serviceability\wsccli.

Accessing the Diagnostic Framework Through the Built-In User Interface (Portico)



Note Starting release 12.6(2), Diagnostic Framework will use only HTTPS to communicate with Framework.

For an end-user to easily harness the functionality of the Diagnostic Framework, a built-in, web-based menu utility called the Diagnostic Framework Portico, allows a user to interact with the framework through their browser. On successful login with the url (<https://localhost:7890/icm-dp/DiagnosticPortal>) it generates an HTML page that can be used to interactively create framework requests and view their replies from the Diagnostic Framework in the same page for the specified server.

Users who do not have access to the Analysis Manager can use this command to gather data from the Diagnostic Framework, without having to know all of the API URLs and parameter values. The Diagnostic Portico Home page recognizes and supports machines with multiple instances [Hosted environment] installed. To access the Diagnostic Framework homepage, no special client side files or installations are needed. You can access the Diagnostic Framework Portico Login page from any machine with a compatible browser.

The entry point for Diagnostic Portico home and menu is through login page. The URL to access is as follows:
`https://localhost:7890/icm-dp/DiagnosticPortal`

Where <UCCE-server> is the hostname or IP address of the desired server, and <port> is the access port (usually 7890).

You can also access the Diagnostic Framework Portico by choosing All Programs > Cisco Unified CCE Tools > Diagnostic Framework Portico.

Most of the commands return simple XML data; the menu utility does some XML parsing and displays the results. A few of these commands create links to allow the user to download the returned files.

The Portico dynamically updates and displays recent changes to processes as below:

- for a process restarted in the last ten minutes, the uptime is underlined and highlighted in red.
- for a process restarted more than 10 minutes ago but less than 30 minutes ago, the uptime is yellow.
- when the status of a process as defined inside the parentheses changes, the process is bolded and highlighted in blue for 10 minutes or until it returns to its former state.

Accessing Diagnostic Framework Commands Through a Browser

Because the Diagnostic Framework is a XML/HTTP based REST-style RPC referred as “RPC-Hybrid” interface, you can access the Diagnostic Framework commands directly through a browser. To access the commands from a browser, type the full URL of the desired command, at the browser address location.

For example, the following URL:

`https://<UCCE-Server>:<port>/icm-dp/rest/DiagnosticPortal/GetTraceLevel?Component=Component/Subcomponent`

The browser displays the data in XML or may ask you to save the file if you are downloading the file. For more information about the URL, see [Diagnostic Framework API, on page 198](#).

The complication with this technique is that there are many APIs, and many of them contain various parameters that you must properly specify.

CLI Configuration

This section will walk you through the configuration required to enter “System mode” and access all devices in your deployment from a single system CLI console window. The CLI supports the following devices:

- All UCCE servers (Routers, Loggers, PGs, ADS, and so on)
- CVP
- CUPS
- Gateways
- UCM
- IP IVR
- CUIC
- Finesse

There are two methods to configuring System mode in the CLI. The method used will depend on whether or not the environment contains CVP OAMP. Customers without CVP OAMP can still utilize the CLI using a CSV file for connection information.

Deployment Option 1: CVP OAMP

CVP OAMP deployment options has several advantages over using Devices.csv including

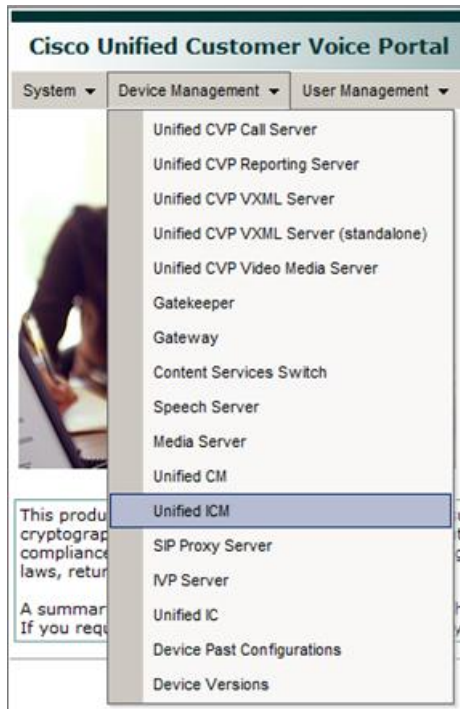
- All devices are centrally added to and stored in CVP OAMP. One update on OAMP will be reflected in all CLI clients.
- Passwords for devices are encrypted in OAMP.
- CVP Remote Operations can be installed on any Windows machine, such as a personal laptop, simplifying setup and access to all devices.

Configure System CLI with CVP OAMP

The first step for setting up System mode is to add all of the devices in your deployment to CVP OAMP.

Procedure

- Step 1** Sign in to CVP Operations Console from a web browser and select **Device Management > Unified ICM**.



Step 2 Click **Add New**.

Step 3 Enter settings for **IP Address**, **Hostname**, and **Description** fields.

 A screenshot of the 'General' tab in the Device Pool configuration form. The form contains the following fields:

- IP Address: * [10.10.10.34]
- Hostname: * [UCCEPG2A34]
- Description: [UCCE MR PG Side A]
- Device Admin URL: []

Step 4 Check **Enable Serviceability**.

Step 5 Enter **Username** and **Password** fields with sign-in credentials for that particular device.

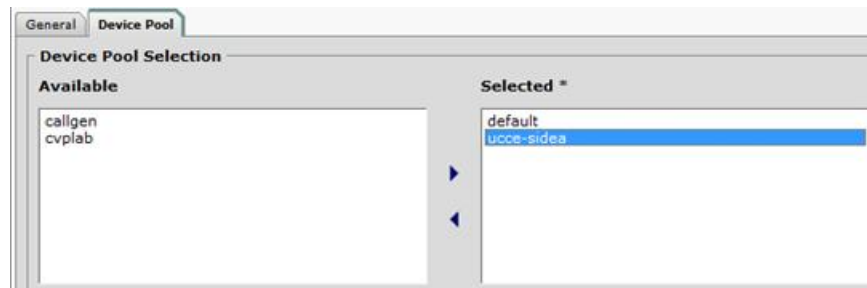
Leave the default port as 7890.

 A screenshot of the 'Enable Serviceability' section in the configuration form. The form contains the following fields:

- Enable Serviceability:
- Username: ¹ [VMLOAD\Administrator]
- Password: ¹ []
- Confirm Password: ¹ []
- Port: ¹ [7890]

Step 6 (Optional) Click **Device Pool** tab and associate the device.

Tip Create a "UCCE-SideA" group for all devices on the A-side.



Step 7 Click **Save**.

What to do next

Repeat the above process for all other devices such as UCCE, CUIC, UCM, Gateways, etc.

Modify or Add User to CVP OAMP for System CLI

By default on installation, the user “wsmadmin” is created with the same password as the OAMP Administrator user. If you wish to modify the password for this user, or create a new user, follow these steps:

Procedure

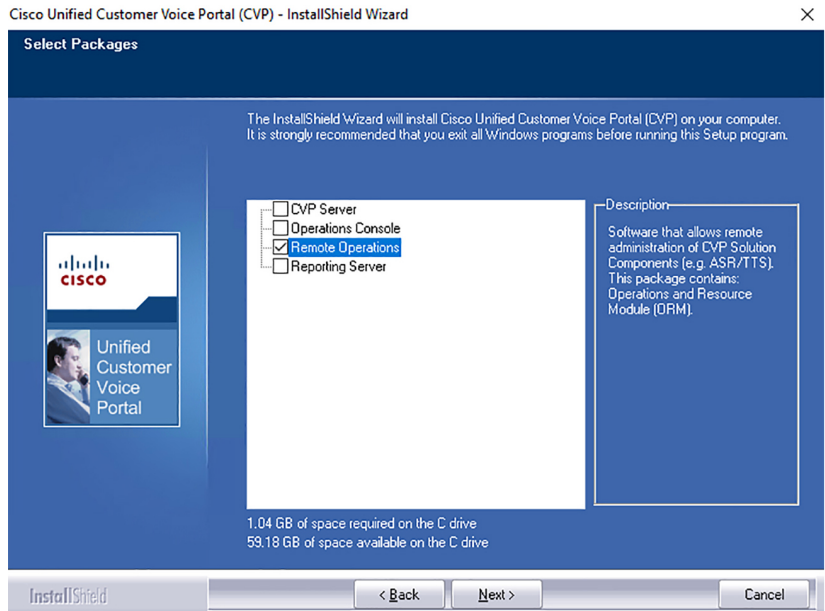
- Step 1** Click **User Management > Users** in CVP Operations Console.
- Step 2** Add or modify user.
- To modify user, click **wsmadmin** in the List of Users.
 - To add user, click **Add New**.
- Step 3** Once new username and/or password has been entered, click **User Groups** tab and add “ServiceabilityAdministrationUserGroup” to “Selected” bucket on right side.
- Step 4** Click **Save**.

Install CVP Remote Operations

Once all devices are added to OAMP, you then need to install the CLI on the system from which you intend to access them. The CVP Installer’s “Remote Operations” package automatically includes the System CLI.

Procedure

- Step 1** Run CVP Installer and select **Remote Operations** checkbox.

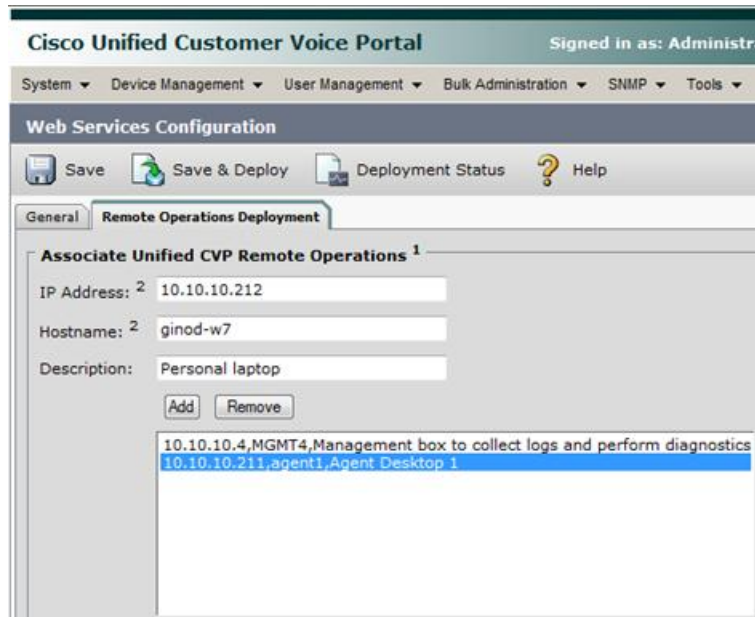


Step 2 Apply security hardening if desired and complete installation.

Add Remote Operations Machines to CVP Operations Console

Procedure

- Step 1** Sign into CVP Operations Console.
- Step 2** Select **System > Web Services**.
- Step 3** Click **Remote Operations Deployment** tab.
- Step 4** Enter remote operations deployment settings for all remote operations machines.



- a) Enter IP address and host name of machine where CVP Remote Operations is installed.
- b) (Optional) Enter description.
- c) Click **Add**.

- Step 5** Click **Save & Deploy** to make devices available for Remote Operations.
You will be informed that the Web Services configuration deployment is in progress.
- Step 6** Click **Deployment Status** button to verify status of newly-added machine(s).
- Step 7** Click **Refresh** button until status changes to “Success”.

Confirm Windows Environment Variables Set Correctly for CVP Web Services

This should have been taken care of by the CVP Remote Operations installation but intermittently fails, so it is important to verify before attempting to connect to the CLI.

Procedure

- Step 1** Click **Start > Run** and enter **systempropertiesadvanced** on the Remote Operations machine.
- Step 2** Click **Environment Variables**.
- Step 3** Verify system variable `WSC_CLI_DIR` is set to `C:\Cisco\CVP\wsm\CLI`.
- Step 4** Verify path variable contains `C:\Cisco\CVP\wsm\CLI;`.

Use Unified System CLI with CVP OAMP

Now that the configuration is finished, you are ready to sign in to the CLI and enter System mode.

Procedure

- Step 1** Select **Start > Programs > Cisco Unified Customer Voice Portal > Unified System CLI** to open Unified System CLI on Remote Operations machine.
- Step 2** Sign in with user “wsmadmin” (or sign in with the new user).
- Step 3** Type **system** to enter System mode.

Servers that are successfully discovered are indicated by a “.”; servers not discovered are indicated by “Unable to connect”. Once initial connection is complete, (system) will be displayed in the command prompt. All commands entered while in System mode will be run against all reachable devices defined in CVP OAMP.

```

Administrator: Unified System CLI
Enter username [wsmadmin]:
Enter password:

Welcome to the Platform Command Line Interface

admin:system
Initializing system mode ...
Retrieving device list. This process may take a few minutes to complete.
.....
admin(system):_

```

What to do next

Any changes made in OAMP while a CLI session is active will not be reflected immediately. There are two options for receiving the updates:

- Close console window and start new connection.
- Type “exit” to leave System mode and then “system init”.

Deployment Option 2: Devices.csv

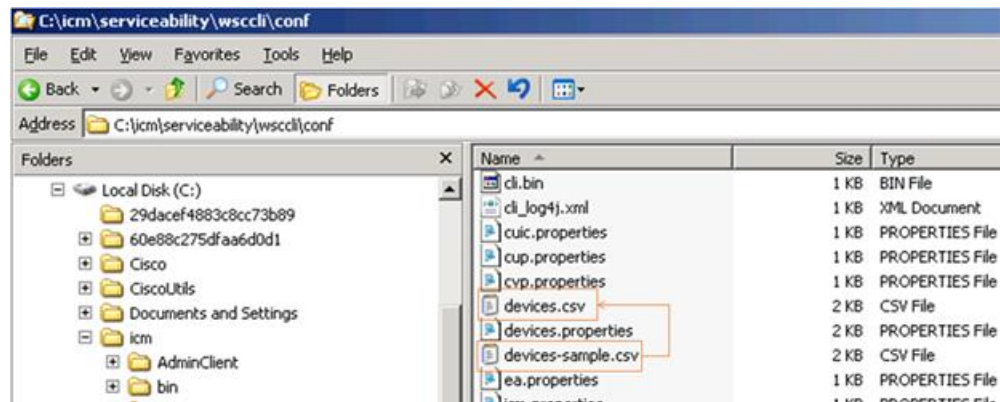
When CVP is not present, Unified System CLI requires a devices.csv file to be configured on the local machine in order to enter System mode. This file contains connection information for all devices in the deployment that should be reachable by the single CLI window.

We will use the ADS as our main machine for running the System CLI.

Create Devices.csv from Sample File

Procedure

- Step 1** Navigate to `C:\icm\serviceability\wsccli\conf\`.
- Step 2** Copy file `devices-sample.csv` and save as `devices.csv`.

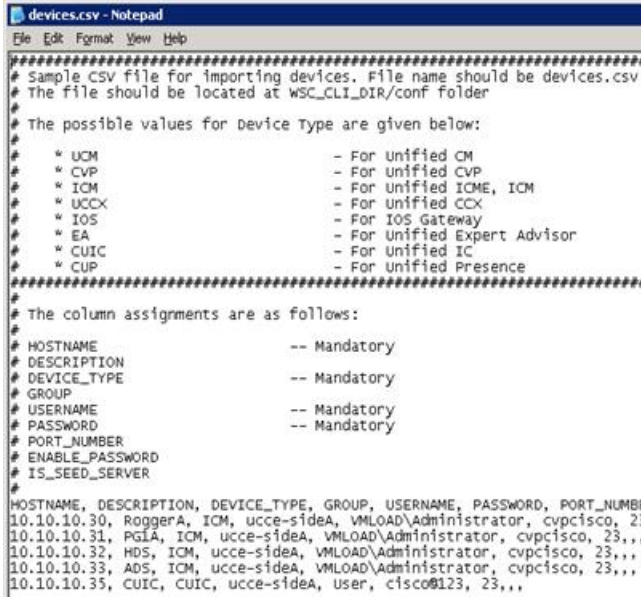


Add Connection Information to Devices.csv File

Each device must be added on its own line at the bottom of the `devices.csv` file.

Procedure

	Command or Action	Purpose
Step 1	<p>Within each line you must specify the following required fields:</p> <ul style="list-style-type: none"> • IP address and hostname • Device Type (from the options listed at the top of the file) • Username • Password • Port Number (leave the default 23 in most cases) 	
Step 2	<p>In addition, specifying the following fields make usage easier:</p> <ul style="list-style-type: none"> • Description • Group (for example, UCCE-SideA) 	

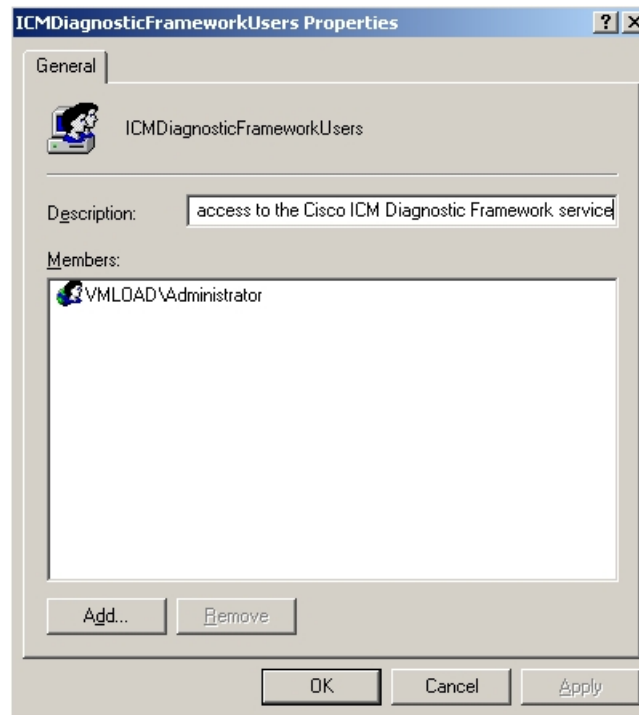
	Command or Action	Purpose
Step 3	Save devices.csv when complete.	 <pre> devices.csv - Notepad File Edit Format View Help ##### # Sample CSV file for importing devices. File name should be devices.csv # The file should be located at %WSC_CLI_DIR%\conf folder # # The possible values for device type are given below: # # * UCM - For Unified CM # * CVP - For Unified CVP # * ICM - For Unified ICME, ICM # * UCCX - For Unified CCX # * IOS - For IOS Gateway # * EA - For Unified Expert Advisor # * CUIC - For Unified IC # * CUP - For Unified Presence ##### # # The column assignments are as follows: # # HOSTNAME -- Mandatory # DESCRIPTION -- Mandatory # DEVICE_TYPE -- Mandatory # GROUP # USERNAME -- Mandatory # PASSWORD -- Mandatory # PORT_NUMBER # ENABLE_PASSWORD # IS_SEED_SERVER # # HOSTNAME, DESCRIPTION, DEVICE_TYPE, GROUP, USERNAME, PASSWORD, PORT_NUMBER 10.10.10.30, RoggerA, ICM, ucce-sideA, VMLOAD\Administrator, cvpcisco, 23,, 10.10.10.31, PGIA, ICM, ucce-sideA, VMLOAD\Administrator, cvpcisco, 23,, 10.10.10.32, HDS, ICM, ucce-sideA, VMLOAD\Administrator, cvpcisco, 23,, 10.10.10.33, ADS, ICM, ucce-sideA, VMLOAD\Administrator, cvpcisco, 23,, 10.10.10.35, CUIC, CUIC, ucce-sideA, user, cisco@123, 23,, </pre>

Designate Users for Diagnostic Framework

Users must be a part of the Local Group “ICMDiagnosticFrameworkUsers” in order to initially sign in to the CLI when using devices.csv.

Procedure

- Step 1** Click **Start > Run**.
- Step 2** Enter “lusrmgr.msc”
- Step 3** Open **Groups** folder and double-click **ICMDiagnosticFrameworkUsers**.
- Step 4** Add users to group and click **OK**.



Use Unified System CLI with Devices.csv

Procedure

- Step 1** Select **Start > Programs > Cisco Unified CCE Tools > Unified System CLI** on ADS.
If this shortcut is missing for some reason, run **C:\icm\serviceability\wsccli\runwsccli.bat**.
- Step 2** Sign in with member of ICMDiagnosticFrameworkUsers group.
If you receive an immediate “Unable to connect to localhost:7890(icm)” error, the Diagnostic Framework service may not be running. Click **Start > Run** and enter **services.msc**. Ensure “Cisco ICM Diagnostic Framework” is started.
- Step 3** Once successfully signed in to local machine, type **system** to enter System mode.
Servers successfully discovered are indicated by a “.” and those that cannot be reached are indicated by “Unable to connect”.

Once initial connection is complete, “(system)” will be displayed in the command prompt. All commands entered while in System mode will be run against all reachable devices defined in devices.csv

```

C:\ Unified System CLI
Enter username (UMLoad\Administrator):
Enter password:
Enter Instance (ucce|Optional):

Welcome to the Platform Command Line Interface

admin:system
Initializing system mode ...
Retrieving device list. This process may take a few minutes to complete.
.....
admin(system):_

```

Running the System CLI from Multiple Machines with Devices.csv

If you intend to run the System CLI on another machine, such as a second ADS, the `devices.csv` file must be copied to that second machine. Any changes made to one `devices.csv` will need to be manually made on the additional machines as well.

Diagnostic Framework API

The Diagnostic Interface supports the following commands.

GetTraceLevel

The Diagnostic Framework supports four levels of trace configuration based on level of trace detail and performance impact; the Diagnostic Framework translates the following levels to component- or process-specific trace level settings:

Table 49: Trace Levels

Trace Level	Description
0	Product/component install default, should have no/minimal performance impact
1	Less detailed trace messages, small performance impact
2	More detailed trace messages, medium performance impact
3	If the trace level does not match any pre-defined levels (for example, a manually configured, specific trace mask), Diagnostic Framework returns “custom (99)”.



Note The minimum and default trace level for the CMS, CMSJServer and ISE components is 2.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/GetTraceLevel?Component=
Component/Subcomponent
```

Reply example:


```
<?xml version="1.0" encoding="UTF-8"?>
<dp:GetTraceLevelReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/diagnosticportal">
<dp:Schema Version="1.0"/>
<dp:Trace Level="0"/>
</dp:GetTraceLevelReply>
```

SetTraceLevel

For more information about the trace level values, see [GetTraceLevel](#), on page 198.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/SetTraceLevel?Component=
Component/Subcomponent&Level=1
```

Reply example:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<dp:SetTraceLevelReply ReturnCode="0"xmlns:dp="http://www.cisco.com/vtg/DiagnosticPortal">
```

```
<dp:Schema Version="1.0"/>
```

```
</dp:SetTraceLevelReply>
```

ListTraceComponents

Lists all possible application components that produce trace files. Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/ListTraceComponents
```

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp>ListTraceComponentsReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/DiagnosticPortal">
<dp:Schema Version="1.0" />
<dp:TraceComponentList>
<dp:TraceComponent Name="Logger A" ComponentType="Logger" Description="ICM Component"
IsLevelConfigurable="true"
IsFileCollectable="true">
<dp:TraceComponentList>
<dp:TraceComponent Name="baImport" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true"
IsFileCollectable="true" />
<dp:TraceComponent Name="CampaignManager" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true" IsFileCollectable="true" />
<dp:TraceComponent Name="clgr" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true"
IsFileCollectable="true" />
```

```

    <dp:TraceComponent Name="csfs" Description="ICM Process for Component LoggerA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="cw2kFeed" Description="ICM Process for Component LoggerA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="dtp" Description="ICM Process for Component LoggerA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="hlgr" Description="ICM Process for Component LoggerA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="nm" Description="ICM Process for Component LoggerA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="nmm" Description="ICM Process for Component LoggerA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="rcv" Description="ICM Process for Component LoggerA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="rpl" Description="ICM Process for Component LoggerA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
  </dp:TraceComponentList>
</dp:TraceComponent>
<dp:TraceComponent Name="Router A" ComponentType="Router" Description="ICM Component"
    IsLevelConfigurable="true"
      IsFileCollectable="true">
  <dp:TraceComponentList>
    <dp:TraceComponent Name="agi" Description="ICM Process for Component RouterA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="ccag" Description="ICM Process for Component RouterA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="dba" Description="ICM Process for Component RouterA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="dbw" Description="ICM Process for Component RouterA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="mds" Description="ICM Process for Component RouterA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="nm" Description="ICM Process for Component RouterA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="nmm" Description="ICM Process for Component RouterA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="nms" Description="ICM Process for Component RouterA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="rtr" Description="ICM Process for Component RouterA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
    <dp:TraceComponent Name="rts" Description="ICM Process for Component RouterA"
    IsLevelConfigurable="true"
      IsFileCollectable="true" />
  </dp:TraceComponentList>
</dp:TraceComponent>
<dp:TraceComponent Name="Cisco ICM Diagnostic Framework" Description="Cisco ICM Diagnostic
Framework"

```

```

    IsLevelConfigurable="true" IsFileCollectable="true" />
<dp:TraceComponent Name="Web Setup" Description="Web Setup" IsLevelConfigurable="true"
IsFileCollectable="true" />
</dp:TraceComponentList>
</dp:ListTraceComponentsReply>

```

ListTraceFiles

Lists trace files for that application component/subcomponent during the FromDate and ToDate parameters (which are in UTC). Request:

```

https://<server>:<port>/icm-dp/rest/DiagnosticPortal/ListTraceFiles?Component/
Subcomponent&FromDate=0&ToDate=0&UseTzadjustoff=NO&Random=1467902083597

```

Reply example:

```

<?xml version="1.0" encoding="UTF-8" ?>
<dp:ListTraceFilesReply ReturnCode="0"
>
<dp:Schema Version="1.0"/>
<dp:TraceFileList>
<dp:FileProperty Name="TraceFile1.TXT" Date="1212347735" Size="1000000"/>
<dp:FileProperty Name="TraceFile2.TXT" Date="1212347835" Size="1000000"/>
<dp:FileProperty Name="TraceFile3.TXT" Date="1212347935" Size="1000000"/>
</dp:TraceFileList>
</dp:ListTraceFilesReply>

```



Note Optional URL parameter Type is applicable only for components that generate multiple trace types.



Note URL parameters FromDate and ToDate are used to specify time range of trace files requested by user. Unified ICM components must supply these parameters.



Note By default value entered in the field UseTzadjustoff is NO. Set the UseTzadjustoff to YES, only if the user is gathering logs across a **Daylight Savings Time**(DST) change.



Note Attribute "Date" specifies file modification time in UTC.



Note Attribute "Size" specifies file size in bytes.

DownloadTraceFile

Download the trace files that were returned by the ListTraceFiles API.



Note Only one file may be requested at a time.

However, for trace files, the ListTraceFiles API returns one zip file (including trace files, capture files, and others). You need only one download request.



Note Subsequent download requests with the same filename return with an error because after the file is downloaded, it is deleted from the server.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/DownloadTraceFile?Component= Component/
Subcomponent&File=TraceFile1.txt
```

Reply:

There are four possible replies:

- The server streams the specified file unzipped over the existing HTTP connection. Content (MIME) type is defined by the app server as “application/text”.
- The server streams the specified file zipped over the existing HTTP connection. Content (MIME) type is defined by app server as “application/zip”.
- The server streams the specified file gzipped over the existing HTTP connection. Content (MIME) type is defined by app server as “application/x-gzip”.
- In case of error, app server replies error condition in following XML format (MIME type “application/xml”):

```
<?xml version="1.0" encoding="UTF-8" ?>
  <dp:DownloadTraceFileReply ReturnCode="1" ErrorString="File TraceFile1.txt not found."/>
  <xmlns:dp="http://www.cisco.com/vtg/diagnosticportal">
```

ListLogComponents

Lists all possible application components that produce log files. Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/ListLogComponents
```

Reply example:

```
<?xml version="1.0" encoding="UTF-8"?>
<dp>ListLogComponentsReply xmlns:dp="http://www.cisco.com/vtg/diagnosticportal"
ReturnCode="0">
<dp:Schema Version="1.0"/>
<dp:LogComponentList>
<dp:LogComponent Description="ICM Installation and Upgrade logs" Name="ICM Installation and
Upgrade"/>
<dp:LogComponent Description="ICM DBA logs" Name="ICMDBA"/>
<dp:LogComponent Description="Performance Counter Logs" Name="Performance Counter"/>
<dp:LogComponent Description="Logs for troubleshooting Active Directory issues." Name="Active
Directory"/>
<dp:LogComponent Description="Cisco ICM Diagnostic Framework Install Logs" Name="Cisco ICM
Diagnostic Framework Install"/>
```

```
<dp:LogComponent Description="Unified System CLI Logs" Name="Unified System CLI"/>
<dp:LogComponent Description="Web Setup logs" Name="Web Setup"/>
<dp:LogComponent Description="Web Setup troubleshooting and audit trail logs" Name="Web
Setup Trail"/>
<dp:LogComponent Description="Tomcat troubleshooting logs" Name="Tomcat"/>
<dp:LogComponent Description="Windows event logs" Name="EventLog"/>
</dp:LogComponentList>
</dp:ListLogComponentsReply>
```

ListLogFiles

Lists log files for that application component/subcomponent during the FromDate and ToDate parameters (which are in UTC). Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/ListLogFiles?Component=
Component/Subcomponent&FromDate=0&ToDate=0
```

Reply example:

```
<?xml version="1.0" encoding="UTF-8"?>
<dp:ListLogFilesReply ReturnCode="0">
<dp:Schema Version="1.0"/>
<dp:LogFileList>
  <dp:FileProperty Name="LogFile1.txt" Date="1212347735" Size="1000000"/>
  <dp:FileProperty Name="LogFile2.txt" Date="1212347835" Size="1000000"/>
  <dp:FileProperty Name="LogFile3.txt" Date="1212347935" Size="1000000"/>
</dp:LogFileList>
</dp:ListLogFilesReply>
```

DownloadLogFile

Download the log files that were returned by the ListLogFiles API.



Note Only one file may be requested at a time.

In the case of downloading the log files, a user may request a subsequent download with the same filename, and the exact same file is returned. This is different from the trace file because we are not deleting the log file from the server.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/DownloadLogFile?Component=Component/Subcomponent&File=LogFile1.txt
```

Reply:

There are four possible replies:

- The server streams the specified file unzipped over the existing HTTP connection. Content (MIME) type is defined by the app server as “application/text”.
- The server streams the specified file zipped over the existing HTTP connection. Content (MIME) type is defined by app server as “application/zip”.
- The server streams the specified file zipped over the existing HTTP connection. Content (MIME) type is defined by app server as “application/x-gzip”.

- In case of error, app server replies error condition in following XML format (MIME type “application/xml”):

```
<?xml version="1.0" encoding="UTF-8" ?>
<dp:DownloadLogFileReply ReturnCode="1" ErrorString="File LogFile1.txt not found."
xmlns:dp="http://www.cisco.com/vtg/diagnosticportal">
```

ListAppServers

Lists the applications and application components installed on the target server. Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/ListAppServers
```

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:ListAppServersReply ReturnCode="0"
>
  <dp:Schema Version="1.0" />
  <dp:AppServerList>
    <dp:AppServer Name="buzzards-bay" ProductType="ICM"
ProductComponentType="Logger A" />
    <dp:AppServer Name="buzzards-bay" ProductType="ICM"
ProductComponentType="Router A" />
    <dp:AppServer Name="buzzards-bay" ProductType="ICM"
ProductComponentType="Cisco ICM Diagnostic Framework" />
  </dp:AppServerList>
</dp:ListAppServersReply>
```

<AppServer> has following optional attributes:

- ProductType: for product to reply topology information. Must be one of the following (“CVP”, “Unified CCX”, “Unified CM”, “Unified CCE”, “EA”, “Cisco IOS Firewall”).
- ProductComponentType: component type within a product. For example: “Router”, “PG”, and so on.

ListConfigurationCategories

Lists the configuration categories available on this application server. Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/ListConfigurationCategories
```

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:ListConfigurationCategoriesReply ReturnCode="0">
  <dp:Schema Version="1.0" />
  <dp:ConfigurationCategoryList>
    <dp:ConfigurationCategory Name="DumpCfg" Description="ConfigurationCategory
for DumpCfg; Instance=acme" />
    <dp:ConfigurationCategory Name="ExportICMCfg"
Description="ConfigurationCategory for ExportICMCfg; Instance=acme" />
    <dp:ConfigurationCategory Name="ConfigExport"
Description="ConfigurationCategory for ConfigExport; Instance=acme" />
    <dp:ConfigurationCategory Name="Registry" Description="ConfigurationCategory
for Registry; Instance=acme" />
  </dp:ConfigurationCategoryList>
</dp:ListConfigurationCategoriesReply>
```

GetConfigurationCategory

Retrieve configuration information based on category. Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/GetConfigurationCategory?Category=<category>
```

Categories are: “DumpCfg”, “ExportICMCfg”, “ConfigExport”, and “Registry”.

Reply example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<dp:GetConfigurationCategoryReply ReturnCode="0">
<dp:Schema Version="1.0"/>
</dp:GetConfigurationCategoryReply>
```

The requested configuration data is returned as a zip file.

GetProductVersion

Fetches the version of the applications installed on the target server.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/GetProductVersion
```

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:GetProductVersionReply ReturnCode="0">
<dp:Schema Version="1.0" />
<dp:ProductVersion Name="ICM" Major="10" Minor="0" Maintenance="1"
  VersionString="10.0(1) BuildNumber=4120" />
</dp:GetProductVersionReply>
```

GetProductLicense

Get license information for applications installed on target server.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/GetProductLicense
```

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:GetProductLicenseReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/diagnosticportal">
<dp:Schema Version="1.0" />
<dp:LicenseList>
  <dp:License>
    <dp:PropertyList>
      <dp:Property Name="License" Value="Unified ICM/Unified CCE does not have any license
information." />
    </dp:PropertyList>
  </dp:License>
</dp:LicenseList>
</dp:GetProductLicenseReply>
```

GetNetStat

Run a NETSTAT command remotely on the target server and return the results.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/GetNetStat?Arguments="-an"
```

Reply:

Returns a text file with the output from the command that was run.

GetIPConfig

Run an IPCONFIG command remotely on the target server and return the results.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/GetIPConfig?Arguments="/all"
```

Reply:

Returns a text file with the output from the command that was run.

GetTraceRoute

Run a TRACERT command remotely on the target server and return the results.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/GetTraceRoute
```

Reply:

Returns a text file with the output from the command that was run.

GetPing

Run a PING command remotely on the target server and return the results.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/GetPing?Arguments="n.n.n.n"
```

Reply:

Returns a text file with the output from the command that was run.

ListProcesses

Lists application processes running on the target server.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/ListProcesses
```


Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:ListProcessesReply ReturnCode="0" xmlns:dp="http://www.cisco.com/vtg/diagnosticportal">
<dp:Schema Version="1.0" />
<dp:ServiceList>
  <dp:Service Name="Logger A">
    <dp:ProcessList>
      <dp:ProcessProp Name="nodeman.exe" Description="nodeman" />
      <dp:ProcessProp Name="nmm.exe" Description="nmm" />
      <dp:ProcessProp Name="configlogger.exe" Description="configlogger" />
      <dp:ProcessProp Name="csfs.exe" Description="csfs" />
      <dp:ProcessProp Name="cw2kfeed.exe" Description="cw2kfeed" />
      <dp:ProcessProp Name="histlogger.exe" Description="histlogger" />
      <dp:ProcessProp Name="recovery.exe" Description="recovery" />
      <dp:ProcessProp Name="replication.exe" Description="replication" />
    </dp:ProcessList>
  </dp:Service>
  <dp:Service Name="Router A">
    <dp:ProcessList>
      <dp:ProcessProp Name="nodeman.exe" Description="nodeman" />
      <dp:ProcessProp Name="nmm.exe" Description="nmm" />
      <dp:ProcessProp Name="ccagent.exe" Description="ccagent" />
      <dp:ProcessProp Name="dbagent.exe" Description="dbagent" />
      <dp:ProcessProp Name="mdsproc.exe" Description="mdsproc" />
      <dp:ProcessProp Name="router.exe" Description="router" />
      <dp:ProcessProp Name="rtsvr.exe" Description="rtsvr" />
      <dp:ProcessProp Name="testsync.exe" Description="testsync" />
    </dp:ProcessList>
  </dp:Service>
  <dp:Service Name="Cisco ICM Diagnostic Framework">
    <dp:ProcessList>
      <dp:ProcessProp Name="DiagFwSvc.exe" Description="DiagFwSvc" />
    </dp:ProcessList>
  </dp:Service>
</dp:ServiceList>
</dp:ListProcessesReply>
```

ListServices

Lists application services running on the target server.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/ListServices
```

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:ListServicesReply ReturnCode="0"
http://www.cisco.com/vtg/diagnosticportal">
<dp:Schema Version="1.0" />
<dp:ServiceList>
  <dp:Service Name="Cisco ICM acme LoggerA" Description="Cisco ICM acme
LoggerA" Status="Running" StartupType="Auto"
LogOnAs="SILVERBACK.CISCO.COM\ACME-LOGGERA-77B585" />
  <dp:Service Name="Cisco ICM acme RouterA" Description="Cisco ICM acme
RouterA" Status="Running" StartupType="Auto" LogOnAs="LocalSystem" />
  <dp:Service Name="Cisco ICM Diagnostic Framework" Description="Provides a
web-based diagnostic service for Cisco Unified ICM,
Enterprise application." Status="Running" StartupType="Auto"
LogOnAs="silverback\w2008admin" />
```

```
</dp:ServiceList>
</dp:ListServicesReply>
```

GetPerformanceInformation

Get a set of System and Application Performance Counters for the specified server.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/GetPerformanceInformation?Component=
Component/Subcomponent
```

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:GetPerformanceInformationReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/diagnosticportal">
<dp:Schema Version="1.0" />
<dp:PerformanceInformation>
<dp:PropertyList>
<dp:Property Name="Memory/Memory Page Faults/sec" Value="29.93962" />
<dp:Property Name="Process(_Total)/Handle Count" Value="20386" />
<dp:Property Name="Processor( _Total)/% Processor Time" Value="13.63913" />
<dp:Property Name="Memory/Total Memory" Value="1.399697E+09" />
<dp:Property Name="System/Threads" Value="1165" />
<dp:Property Name="Memory/Memory Pages/Sec" Value="3.654335" />
<dp:Property Name="System/Processor Queue" Value="0" />
<dp:Property Name="System/Processes" Value="73" />
<dp:Property Name="Cisco ICM Logger(acme LoggerA)/DB Write Average Time" Value="0" />
<dp:Property Name="Cisco ICM Logger(acme LoggerA)/DB Write Records processed" Value="0"
/>
<dp:Property Name="Cisco ICM Router(acme RouterA)/Calls/sec" Value="0" />
<dp:Property Name="Cisco ICM Router(acme RouterA)/Agents Logged On" Value="0" />
<dp:Property Name="Cisco ICM Router(acme RouterA)/Calls In Progress" Value="0" />
<dp:Property Name="Cisco ICM Router(acme RouterA)/Calls In Queue" Value="0" />
<dp:Property Name="Cisco ICM Router(acme RouterA)/Router State Size(KB)" Value="0" />
<dp:Property Name="Cisco ICM Router(acme RouterA)/Messages Processed/sec" Value="0" />
<dp:Property Name="Cisco ICM Router(acme RouterA)/Bytes Processed/sec" Value="0" />
<dp:Property Name="Cisco ICM Router(acme RouterA)/Avg Process Time/Message (ms)" Value="0"
/>
<dp:Property Name="Cisco ICM Router(acme RouterA)/Max Process Time(ms)" Value="0" />
<dp:Property Name="Cisco ICM Router(acme RouterA)/Calls In Router" Value="0" />
</dp:PropertyList>
</dp:PerformanceInformation>
</dp:GetPerformanceInformationReply>
```

GetPerfCounterValue

Get the current value of a performance counter from the target server.

Request

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/GetPerfCounterValue?
CategoryName=Processor&CounterName="%Processor Time"&PerfInstance="_Total"
```

Reply Example

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:GetPerfCounterValueReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/diagnosticportal">
<dp:Schema Version="1.0" />
<dp:PerformanceInformation>
<dp:PropertyList>
  <dp:Property Name="CategoryName" Value="Processor" />
  <dp:Property Name="CounterName" Value="% Processor Time" />
  <dp:Property Name="InstanceName" Value="_Total" />
  <dp:Property Name="BaseValue" Value="0" />
  <dp:Property Name="CounterFrequency" Value="0" />
  <dp:Property Name="CounterTimeStamp" Value="0" />
  <dp:Property Name="CounterType" Value="Timer100NsInverse" />
  <dp:Property Name="RawValue" Value="203276171875" />
  <dp:Property Name="NextValue" Value="0.003199898" />
  <dp:Property Name="SystemFrequency" Value="2333380000" />
  <dp:Property Name="TimeStamp" Value="48917923479390" />
  <dp:Property Name="TimeStamp100nSec" Value="128929442042854145" />
</dp:PropertyList>
</dp:PerformanceInformation>
</dp:GetPerfCounterValueReply>
```

GetAlarms

Retrieves up to 25 of the most recent alarms generated by the Unified CCE.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/GetAlarms?Severity=
#?Count=##
```

Severity and Count are optional parameters. Severity may be a numeric value between “1” and “3” (“1”=Informational, “2”=Warning, “3”=Error). Severity returns all alarms with a severity greater-than or equal-to the specified severity. Count may be a numeric value between “1” and “25”. Count returns a maximum of the specified number of alarms.

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:GetAlarmsReply ReturnCode="0" xmlns:dp="http://www.cisco.com/vtg/diagnosticportal">
<dp:Schema Version="1.0" />
<dp:AlarmList>
  <dp:Alarm DateTime="Jul 24, 2009 15:41:41 +0000" Type="Clear" Id="1028104" Severity="1"
Instance="acme"
Component="4_5_BERKSHIRE_ICM\acme\LoggerB" SubComponent="nm" Message="ICM\acme\LoggerB Node
Manager started. Last
shutdown was due to system shutdown." />
  <dp:Alarm DateTime="Jul 24, 2009 15:41:27 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_hlgr" SubComponent="rtr" Message="Side B hlgr process is OK." />
  <dp:Alarm DateTime="Jul 24, 2009 15:42:37 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_clgr" SubComponent="rtr" Message="Side B clgr process is OK." />
  <dp:Alarm DateTime="Jul 24, 2009 15:41:27 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_clgr" SubComponent="rtr" Message="Side B clgr process is OK." />
  <dp:Alarm DateTime="Jul 24, 2009 15:41:14 +0000" Type="Clear" Id="10F8004" Severity="1"
```

```

Instance="acme"
Component="6_1_BERKSHIRE_B_PG01" SubComponent="ccag" Message="Device PG01 path changing to
idle state." />
<dp:Alarm DateTime="Jul 24, 2009 15:41:14 +0000" Type="Clear" Id="102C107" Severity="1"
Instance="acme"
Component="4_1_BERKSHIRE_ICM\acme\RouterB" SubComponent="nm" Message="ICM\acme\RouterB Node
Manager started. Last
shutdown was for reboot after failure of critical process." />
<dp:Alarm DateTime="Jul 24, 2009 15:41:13 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_rts" SubComponent="rtr" Message="Side B rts process is OK." />
<dp:Alarm DateTime="Jul 24, 2009 15:41:12 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_rtr" SubComponent="rtr" Message="Side B rtr process is OK." />
<dp:Alarm DateTime="Jul 24, 2009 15:41:12 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_tsy" SubComponent="rtr" Message="Side B tsyr process is OK." />
<dp:Alarm DateTime="Jul 24, 2009 15:41:12 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_csfs" SubComponent="rtr" Message="Side B csfs process is OK." />
<dp:Alarm DateTime="Jul 24, 2009 15:41:12 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_rcv" SubComponent="rtr" Message="Side B rcv process is OK." />
<dp:Alarm DateTime="Jul 24, 2009 15:41:12 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_dba" SubComponent="rtr" Message="Side B dba process is OK." />
<dp:Alarm DateTime="Jul 24, 2009 15:42:20 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_rtr" SubComponent="rtr" Message="Side B rtr process is OK." />
<dp:Alarm DateTime="Jul 24, 2009 15:42:20 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_tsy" SubComponent="rtr" Message="Side B tsyr process is OK." />
<dp:Alarm DateTime="Jul 24, 2009 15:42:20 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_csfs" SubComponent="rtr" Message="Side B csfs process is OK." />
<dp:Alarm DateTime="Jul 24, 2009 15:42:20 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_rcv" SubComponent="rtr" Message="Side B rcv process is OK." />
<dp:Alarm DateTime="Jul 24, 2009 15:42:20 +0000" Type="Clear" Id="10500FF" Severity="1"
Instance="acme"
Component="24_1_B_dba" SubComponent="rtr" Message="Side B dba process is OK." />
<dp:Alarm DateTime="Jul 24, 2009 15:42:18 +0000" Type="Clear" Id="1040023" Severity="1"
Instance="acme"
Component="5_1_0" SubComponent="mds" Message="Communication with peer Synchronizer
established." />
<dp:Alarm DateTime="Jul 24, 2009 15:37:55 +0000" Type="Clear" Id="1028103" Severity="1"
Instance="acme"
Component="4_4_WACHUSETT_ICM\acme\Distributor" SubComponent="nm" Message="ICM\acme\Distributor
Node Manager
started. Last shutdown was by operator request." />
<dp:Alarm DateTime="Jul 24, 2009 15:37:41 +0000" Type="Clear" Id="102C110" Severity="2"
Instance="acme"
Component="3_4_WACHUSETT_ICM\acme\Distributor_uaw" SubComponent="nm"
Message="ICM\acme\Distributor node process
uaw successfully reinitialized after restart." />
<dp:Alarm DateTime="Jul 24, 2009 15:37:40 +0000" Type="Clear" Id="102C10A" Severity="2"
Instance="acme"
Component="3_4_WACHUSETT_ICM\acme\Distributor_uaw" SubComponent="nm"
Message="ICM\acme\Distributor node restarting
process uaw after having delayed restart for 1 seconds." />
<dp:Alarm DateTime="Jul 24, 2009 15:37:39 +0000" Type="Raise" Id="102C10F" Severity="2"
Instance="acme"
Component="3_4_WACHUSETT_ICM\acme\Distributor_uaw" SubComponent="nm" Message="Process uaw
on ICM\acme\Distributor

```

```

is down after running for 30 seconds. It will restart after
    delaying 1 second for related operations to complete." />
<dp:Alarm DateTime="Jul 24, 2009 15:37:39 +0000" Type="Raise" Id="102C10E" Severity="3"
Instance="acme"
Component="3_4_WACHUSETT_ICM\acme\Distributor_uaw" SubComponent="nm" Message="Process uaw
on ICM\acme\Distributor
went down for unknown reason. Exit code 0x1. It will be
    automatically restarted." />
<dp:Alarm DateTime="Jul 24, 2009 15:37:14 +0000" Type="Clear" Id="102C111" Severity="1"
Instance="acme"
Component="3_4_WACHUSETT_ICM\acme\Distributor_rpl" SubComponent="nm"
Message="ICM\acme\Distributor node process
rpl successfully started." />
<dp:Alarm DateTime="Jul 24, 2009 15:37:13 +0000" Type="Clear" Id="102C111" Severity="1"
Instance="acme"
Component="3_4_WACHUSETT_ICM\acme\Distributor_rtc" SubComponent="nm"
Message="ICM\acme\Distributor node process
rtc successfully started." />
</dp:AlarmList>
</dp:GetAlarmsReply>

```

SetAlarms

Turns the Unified CCE alarming OFF or ON. Turning the alarming OFF is useful during maintenance windows to prevent flooding at the management station.

Request:

```
https://<server>:<port>/icm-dp/rest/DiagnosticPortal/SetAlarms?State=ON/OFF
```

Reply example:

```

<?xml version="1.0" encoding="utf-8" ?>
<dp:SetAlarmsReply ReturnCode="0"
>
<dp:Schema Version="1.0" />
</dp:SetAlarmsReply>

```

SNMP/Syslog REST API

The Unified CCE SNMP implementation includes a set of SNMP agents (one primary and a set of subagents), and a service that manages the agent infrastructure. The SNMP primary agent is configured using a Microsoft Management Console (MMC) snap-in application that provides a simple user interface.

This user interface does the following:

- configuration parameters from the user
- saves the parameters
- signals the management service to restart the agents

These tasks can also be accomplished using the REST APIs for Community, User, and Traps properties.

General Information

The General Information API allows you to configure system level information that can be fetched by any NMS that query a particular instrumentation. It also adds restrictions to various sub agents that can be loaded by the SNMP primary agent.

The default port to get any instrumentation detail is 161. You can change this port by using the General Information API. You can also use the General Information API to set the SNMP log trace level.

Both SNMP and SysLog use some part of the General information API. For more information, see *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise*.

Get

This implementation of the SNMP GeneralInfo string retrieves the details of the General Information API.

Table 50: Parameters of General Information API String Get

URL	https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/GeneralInfo
HTTP Method	GET
Input/Output Format	XML
Request	The GET operation on the service endpoint retrieves the details of the SNMP General Information. GET https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/GeneralInfo
Content-type	Application/XML
Accept	Application/XML
Request Data Structure	In this implementation, the user sends the identifier in the request path parameter.
Response Data Structure	<pre><?xml version="1.0" encoding="utf-8"?> <dp:GeneralInformationReply ReturnCode="0"> <dp:Schema Version="1.0"/> <dp:GeneralInformation> <dp:systemName>user_name</dp:systemName> <dp:systemLocation>----</dp:systemLocation> <dp:systemContact>----</dp:systemContact> <dp:systemDescription>Cisco Contact Center Application Server</dp:systemDescription> <dp:agentPollsPort>1</dp:agentPollsPort> <dp:enableAuthenticationTraps>>false</dp:enableAuthenticationTraps> <dp:agentExecutionPriority>1</dp:agentExecutionPriority> <dp:maximumConcurrentRequests>5</dp:maximumConcurrentRequests> <dp:maximumSubagentWaitTime>25</dp:maximumSubagentWaitTime> <dp:maximumSubagents>25</dp:maximumSubagents> <dp:agentLogQuantity>1</dp:agentLogQuantity> </dp:GeneralInformation> </dp:GeneralInformationReply></pre>
Response Header	Return 200 OK. Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0

Response Code	<p>400- Bad request. If the request body is invalid.</p> <p>400- API error . If the object either does not exist or is stale.</p> <p>403- Authorization Failure (for example, the user is not authenticated in the web session).</p> <p>500- Internal Server Error. This error is displayed for all generic server side errors. Details about the error will be given in the error notification that is displayed in the response body.</p> <p>503 Service Unavailable. When the request processing threshold is reached.</p>
Security Constraints	Only a Serviceability administrator can perform this operation.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value
systemName	Represents the host name (or fully qualified domain name).	String	Length <= 127	No	Alphanumeric
systemLocation	Represents the physical location of this host.	String	Length <= 127	No	Alphanumeric
systemContact	Represents the name of the person to contact if a problem arises with this host.	String	Length <= 127	No	Alphanumeric
systemDescription	Represents the Description of this host(any information deemed relevant).	String	Length <= 127	No	Alphanumeric
agentPollsPort	Represents the port number that the SNMP primary agent listens for inbound requests.	String	Length <= 5	No	Numeric
enableAuthenticationTraps	When enabled, sends a trap when an authentication failure occurs.	Boolean	-	No	true /false; case sensitive
agentExecutionPriority	Represents the thread execution priority for all SNMP agents.	Int	0-2	No	-
maximumConcurrentRequests	Represents the maximum concurrent SNMP Objects request that are allowed.	Unsigned Int	2-32	No	-
maximumSubagentWaitTime	Represents the maximum number of seconds a primary agent will wait for a subagent to respond to a request (timeout).	Unsigned Int	5-150	No	
maximumSubagents	Represents the maximum number of SNMP subagents the primary agent permits to be loaded.	Unsigned Int	5-150	No	
agentLogQuantity	Represents the number of log messages to be written to the agent log files.	Int	0-2	No	

Update

This implementation of the SNMP GeneralInfo string updates the properties of the General Information API.

Table 51: Parameters of General Information API String Update

URL	https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/GeneralInfo
HTTP Method	PUT
Input/Output Format	XML
Request	The PUT operation on the service endpoint updates the properties of the General Information API. PUT https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/GeneralInfo
Content-type	Application/XML
Accept	Application/XML
Request Data Structure	<pre><GeneralInformation> <systemName>MachineName.MachineDomain.instance</systemName> <systemLocation>-</systemLocation> <systemContact>-</systemContact> <systemDescription>Cisco Contact Center Application Server</systemDescription> <agentPollsPort>1</agentPollsPort> <enableAuthenticationTraps>>false</enableAuthenticationTraps> <agentExecutionPriority>1</agentExecutionPriority> <maximumConcurrentRequests>5</maximumConcurrentRequests> <maximumSubagentWaitTime>25</maximumSubagentWaitTime> <maximumSubagents>25</maximumSubagents> <agentLogQuantity>2</agentLogQuantity> </GeneralInformation></pre>
Response Header	Return 200 OK. Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0
Response Code	400- Bad request. If the request body is invalid. 400- API error . If the object either does not exist or is stale. 403- Authorization Failure (for example, the user is not authenticated in the web session). 500- Internal Server Error. This error is displayed for all generic server side errors. Details about the error will be given in the error notification that is displayed in the response body. 503 Service Unavailable. When the request processing threshold is reached.
Security Constraints	Only a Serviceability administrator can perform this operation.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value
systemName	Represents the host name (or fully qualified domain name).	String	Length <= 127	No	Alphanumeric

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value
systemLocation	Represents the physical location of this host.	String	Length <= 127	No	Alphanumeric
systemContact	Represents the name of the person to contact if a problem arises with this host.	String	Length <= 127	No	Alphanumeric
systemDescription	Represents the Description of this host(any information deemed relevant).	String	Length <= 127	No	Alphanumeric
agentPollsPort	Represents the port number that the SNMP primary agent listens for inbound requests.	String	Length <= 5	No	-
enableAuthenticationTraps	When enabled, sends a trap when an authentication failure occurs.	Boolean	-	No	true/false; case sensitive
agentExecutionPriority	Represents the thread execution priority for all SNMP agents.	Int	0-2	No	-
maximumConcurrentRequests	Represents the maximum concurrent SNMP Objects request that are allowed.	Unsigned Int	2-32	No	-
maximumSubagentWaitTime	Represents the maximum number of seconds a primary agent will wait for a subagent to respond to a request (timeout).	Unsigned Int	5-150	No	
maximumSubagents	Represents the maximum number of SNMP subagents the primary agent permits to be loaded.	Unsigned Int	5-150	No	
agentLogQuantity	Represents the number of log messages to be written to the agent log files.	Int	0-2	No	

SNMP v1/v2c Community

If you are using SNMP v1 or v2c you must configure a community name so that Network Management Stations (NMS) can access the data provided by your server. These names are left blank during installation for security reasons.

SNMP community names are used to authenticate data exchange of SNMP information. An NMS can exchange SNMP information only with servers that use the same community name.



Note SNMP community name along with the SNMP Version forms an unique entity and acts as a primary key.

Create

This implementation of SNMP v1/v2c community string creates a SNMP community mentioned in the request.

Table 52: Parameters of SNMP v1/v2c Community String Create

URL	https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/community
HTTP Method	POST
Input/Output Format	XML
Request	The POST operation on the service endpoint creates the SNMP Community. POST https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/community
Content-type	Application/XML
Accept	Application/XML
Request Data Structure	<?xml version="1.0" encoding="utf-8"?> <community> <name>Public_Community</name> <snmpversion>V1</snmpversion> <accessprivilege>ReadOnly</accessprivilege> <hosts> <host>192.0.2.0</host> </hosts> </community>
Response Header	Return 201 CREATED. Response headers: HTTP/1.1 201 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0 Date: Mon, 26 Aug 2013 09:15:27 GMT
Response Code	400- Bad request. If the request body is invalid. 400- API error . If the object either does not exist or is stale. 403- Authorization Failure (for example, the user is not authenticated in the web session). 500- Internal Server Error. This error is displayed for all generic server side errors. Details about the error will be given in the error notification that is displayed in the response body. 503 Service Unavailable. When the request processing threshold is reached.
Security Constraints	Only a Serviceability administrator can perform this operation.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
name	Represents the community string name	String	Length <= 40	Yes	Alphanumeric	Alphanumeric dot, underscore, and hyphens are allowed. Space is not allowed.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
snmpversion	Represents the SNMP version information	String	-	No	V1 (default), V2c	Only V1 or V2c; Not case sensitive.
hosts	Represents a list of "host" tags	-	-	No	If this tag is specified, then the host tag is mandatory.	-
host	Represents the management station host IP address. If the management station host IP address is not provided then any host can request for the management information.	String	Valid IP address; number of host tags must be <= 255	No	A valid ip4 address	-
accessprivilege	Represents the access privileges of the community string.	String	-	No	ReadOnly (default), ReadWrite	Only ReadOnly or ReadWrite; Not case sensitive.

Delete

This implementation of SNMP v1/v2c community string deletes the community from the listed devices.

Table 53: Parameters of SNMP v1/v2c Community String Delete

URL	DELETE https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/community/Name/<name>&SnmVersion/<snmpversion>
HTTP Method	DELETE
Input/Output Format	XML
Request	The DELETE operation on the service endpoint deletes the SNMP Community. DELETE https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/community/Name/<name>&SnmVersion/<snmpversion>
Content-type	Application/XML
Accept	Application/XML
Request Data Structure	In this implementation, the user sends the identifier in the request path parameter.
Response Header	Return 200 OK. Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0

Response Code	<p>400- Bad request. If the request body is invalid.</p> <p>400- API error . If the object either does not exist or is stale.</p> <p>403- Authorization Failure (for example, the user is not authenticated in the web session).</p> <p>500- Internal Server Error. This error is displayed for all generic server side errors. Details about the error will be given in the error notification that is displayed in the response body.</p> <p>503 Service Unavailable. When the request processing threshold is reached.</p>
Security Constraints	Only a Serviceability administrator can perform this operation.

Get

This implementation of the SNMP v1/v2c community string retrieves the details of the community.

Table 54: Parameters of SNMP v1/v2c Community String Get

URL	<p>GET</p> <p><code>https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/community/Name/<name>&SnmVersion/<snmpversion></code></p>
HTTP Method	GET
Input/Output Format	XML
Request	<p>The GET operation on the service endpoint retrieves the details of the SNMP community.</p> <p>GET</p> <p><code>https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/community/Name/<name>&SnmVersion/<snmpversion></code></p>
Content-type	Application/XML
Accept	Application/XML
Request Data Structure	In this implementation, the user sends the identifier in the request path parameter.
Response Data Structure	<pre><?xml version="1.0" encoding="utf-8"?> <dp:CommunityReply ReturnCode="0" xmlns:dp="http://www.cisco.com/vtg/diagnosticportal"> <dp:Schema Version="1.0" /> <dp:community> <dp:name>str1</dp:name> <dp:snmpversion>V2c</dp:snmpversion> <dp:accessprivilege>ReadOnly</dp:accessprivilege> <dp:hosts> <dp:host>192.0.2.0</dp:host> <dp:host>192.0.2.1</dp:host> </dp:hosts> </dp:community> </dp:CommunityReply></pre>
Response Header	<p>Return 200 OK.</p> <p>Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0</p>

Response Code	<p>400- Bad request. If the request body is invalid.</p> <p>400- API error . If the object either does not exist or is stale.</p> <p>403- Authorization Failure (for example, the user is not authenticated in the web session).</p> <p>500- Internal Server Error. This error is displayed for all generic server side errors. Details about the error will be given in the error notification that is displayed in the response body.</p> <p>503 Service Unavailable. When the request processing threshold is reached.</p>
Security Constraints	Only a Serviceability administrator can perform this operation.

List

This implementation of SNMP v1/v2c community string lists all the communities that are configured on the system.

Table 55: Parameters of SNMP v1/v2c Community String List

URL	<code>https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/community</code>
HTTP Method	GET
Input/Output Format	XML
Request	<p>The GET operation on the service endpoint lists the details of the SNMP community.</p> <p>GET <code>https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/community</code></p>
Content-type	Application/XML
Accept	Application/XML
Response Data Structure	<pre><?xml version="1.0" encoding="utf-8"?> <dp:CommunityReply ReturnCode="0" xmlns:dp="http://www.cisco.com/vtg/diagnosticportal"> <dp:Schema Version="1.0" /> <dp:communities> <dp:community> <dp:name>george</dp:name> <dp:snmpversion>V1</dp:snmpversion> </dp:community> <dp:community> <dp:name>public_community</dp:name> <dp:snmpversion>V2c</dp:snmpversion> </dp:community> </dp:communities> </dp:CommunityReply></pre>
Response Header	<p>Return 200 OK.</p> <p>Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0</p>

Response Code	<p>400- Bad request. If the request body is invalid.</p> <p>400- API error . If the object either does not exist or is stale.</p> <p>403- Authorization Failure (for example, the user is not authenticated in the web session).</p> <p>500- Internal Server Error. This error is displayed for all generic server side errors. Details about the error will be given in the error notification that is displayed in the response body.</p> <p>503 Service Unavailable. When the request processing threshold is reached.</p>
Security Constraints	Only a Serviceability administrator can perform this operation.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
name	Represents the community string name	String	Length <= 40	Yes	Alphanumeric	Alphanumeric dot, underscore, and hyphens are allowed. Space is not allowed.
snmpversion	Represents the SNMP version information	String	-	No	V1 (default), V2c	Only V1 or V2c; Not case sensitive.

Update

This implementation of SNMP v1/v2c community string updates the properties of the SNMP community string.

Only full update of SNMP v1/v2c Community API is allowed. Therefore, all the XML tags with valid values must be included while sending the update request. For more information, see [Update Implementation for SNMP/Syslog REST APIs, on page 239](#).

Table 56: Parameters of SNMP v1/v2c Community String Update

URL	<code>https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/community</code>
HTTP Method	PUT
Input/Output Format	XML
Request	<p>The PUT operation on the service endpoint updates the properties of the SNMP community.</p> <p>PUT <code>https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/community</code></p>
Content-type	Application/XML
Accept	Application/XML
Request Data Structure	<pre><?xml version="1.0" encoding="utf-8"?> <community> <name>Public_Community</name> <snmpversion>V1</snmpversion> <accessprivilege>ReadOnly</accessprivilege> <hosts> <host>192.0.2.0</host> </hosts> </community></pre>

Response Header	Return 200 OK. Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0
Response Code	400- Bad request. If the request body is invalid. 400- API error . If the object either does not exist or is stale. 403- Authorization Failure (for example, the user is not authenticated in the web session). 500- Internal Server Error (for example, the connection is broken with the database server or ORM or any other component. 503 Service Unavailable. When the request processing threshold is reached.
Security Constraints	Only a Serviceability administrator can perform this operation.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
name	Represents the community string name	String	Length <= 40	Yes	Alphanumeric	Alphanumeric dot, underscore, and hyphens are allowed. Space is not allowed.
snmpversion	Represents the SNMP version information	String	-	Yes	V1 (default), V2c	Only V1 or V2c; Not case sensitive.
hosts	Represents a list of "host" tags	-	-	Yes	If this tag is specified, then the host tag is mandatory.	-
host	Represents the management station host IP address. If the management station host IP address is not provided then any host can request for the management information.	String	Valid IP address; number of host tags must be <= 255	Yes	A valid ip4 address	-
accessprivilege	Represents the access privileges of the community string.	String	-	Yes	ReadOnly (default), ReadWrite	Only ReadOnly or ReadWrite; Not case sensitive.

SNMPv3 User

If you are using Simple Network Management Protocol Version 3 (SNMPv3) you must configure a user name so that the Network Management Stations (NMS) can access the data provided by your server.

Create

This implementation of SNMP user string creates an SNMP user as mentioned in the request.

Table 57: Parameters of SNMP User String Create

URL	https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/user
HTTP Method	POST
Input/Output Format	XML
Request	The POST operation on the service endpoint creates the SNMP User. POST https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/user
Content-type	Application/XML
Accept	Application/XML
Request Data Structure	<pre><?xml version="1.0" encoding="UTF-8" standalone="yes"?> <user> <name>Snm_User</name> <accessprivilege>ReadOnly</accessprivilege> <hosts> <host>192.0.2.0</host> </hosts> <authInfoReqd>true</authInfoReqd> <authProtocol>MD5</authProtocol> <authPassword>user@123</authPassword> <privacyInfoReqd>true</privacyInfoReqd> <privacyProtocol>AES-192</privacyProtocol> <privacyPassword>user@123456</privacyPassword> </user></pre>
Response Header	Return 201 CREATED. Response headers: HTTP/1.1 201 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0 Date: Mon, 26 Aug 2013 09:15:27 GMT
Response Code	400- Bad request. If the request body is invalid. 400- API error. If the object either does not exist or is stale. 403- Authorization Failure (for example, the user is not authenticated in the web session). 500- Internal Server Error. This error is displayed for all generic server-side errors. Details about the error is given in the error notification that is displayed in the response body. 503 Service Unavailable. When the request processing threshold is reached.
Security Constraints	Only a Serviceability administrator can perform this operation.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
name	Represents the user string name.	String	Length <= 40	Yes	Alphanumeric	Alphanumeric dot, underscore, and hyphens are allowed. Space is not allowed.
accessprivilege	Represents the access privileges of the user string.	String	-	No	ReadOnly (default), ReadWrite	Only ReadOnly or ReadWrite; Not case sensitive.
hosts	Represents a list of "host" tags.	-	-	No	If this tag is specified, then the host tag is mandatory.	-
host	Represents the management station host IP address. If the management station host IP address is not provided, then any host can request for the management information.	String	Valid IP address; number of host tags must be <= 255	No	A valid ip4 address	-
authInfoReqd	Authentication information is required.	Boolean	-	No. If this tag is not provided, then the default value, false, will be considered.	false, true	Case sensitive.
authProtocol	Authentication protocol.	String	-	No. If authInfoReqd is true, then this field is mandatory.	MD5 SHA-1	Value for this tag is set only when authInfoReqd is true.
authPassword	Authentication password.	String	-	No. If authInfoReqd is true, then this field is mandatory.	Alphanumeric with any special character.	Value for this tag is set only when authInfoReqd is true.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
privacyInfoReqd	Privacy information is required.	Boolean	-	No.	false, true	Case sensitive. If privacyInfoReqd is true, then authInfoReqd must be set to true.
privacyProtocol	Privacy protocol.	String	-	No. If privacyInfoReqd is true, then this field is mandatory.	3DES AES-192 AES-256	Value for this tag is set only when privacyInfoReqd is true.
privacyPassword	Privacy password.	String	-	No. If privacyInfoReqd is true, then this field is mandatory.	Alphanumeric with any special character.	Value for this tag is set only when privacyInfoReqd is true.

Delete

This implementation of SNMP user string deletes the user from the listed devices.

Table 58: Parameters of SNMP User String Delete

URL	DELETE https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/user/Name/<name>
HTTP Method	DELETE
Input/Output Format	XML
Request	The DELETE operation on the service endpoint deletes the SNMP User. DELETE https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/user/Name/<name>
Content-type	Application/XML
Accept	Application/XML
Request Data Structure	In this implementation, the user sends the identifier in the request path parameter.
Response Header	Return 200 OK. Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0

Response Code	<p>400- Bad request. If the request body is invalid.</p> <p>400- API error. If the object either does not exist or is stale.</p> <p>403- Authorization Failure (for example, the user is not authenticated in the web session).</p> <p>500- Internal Server Error. This error is displayed for all generic server-side errors. Details about the error is given in the error notification that is displayed in the response body.</p> <p>503 Service Unavailable. When the request processing threshold is reached.</p>
Security Constraints	Only a Serviceability administrator can perform this operation.

Get

This implementation of the SNMP user string retrieves the details of the user.

Table 59: Parameters of SNMP User String Get

URL	GET https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/user/Name/<name>
HTTP Method	GET
Input/Output Format	XML
Request	<p>The GET operation on the service endpoint retrieves the details of the SNMP User.</p> <p>GET https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/user/Name/<name></p>
Content-type	Application/XML
Accept	Application/XML
Request Data Structure	In this implementation, the user sends the identifier in the request path parameter.
Response Data Structure	<pre><dp:UserReply ReturnCode="0"> <dp:Schema Version="1.0"/> <dp:user> <dp:name>Snmp_User</dp:name> <dp:accessprivilege>ReadOnly</dp:accessprivilege> <dp:hosts> <dp:host>192.0.2.0</dp:host> </dp:hosts> <dp:authInfoReqd>true</dp:authInfoReqd> <dp:authProtocol>MD5</dp:authProtocol> <dp:privacyInfoReqd>true</dp:privacyInfoReqd> <dp:privacyProtocol>AES-192</dp:privacyProtocol> </dp:user> </dp:UserReply></pre>
Response Header	<p>Return 200 OK.</p> <p>Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0</p>

Response Code	<p>400- Bad request. If the request body is invalid.</p> <p>400- API error. If the object either does not exist or is stale.</p> <p>403- Authorization Failure (for example, the user is not authenticated in the web session).</p> <p>500- Internal Server Error. This error is displayed for all generic server-side errors. Details about the error will be given in the error notification that is displayed in the response body.</p> <p>503 Service Unavailable. When the request processing threshold is reached.</p>
Security Constraints	Only a Serviceability administrator can perform this operation.

List

This implementation of SNMP User string lists all the users that are configured on the system.

Table 60: Parameters of SNMP User String List

URL	<code>https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/user</code>
HTTP Method	GET
Input/Output Format	XML
Request	<p>The GET operation on the service endpoint lists the details of the SNMP User.</p> <p>GET <code>https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/user</code></p>
Content-type	Application/XML
Accept	Application/XML
Response Data Structure	<pre><dp:ListUserReply ReturnCode="0"> <dp:Schema Version="1.0"/> <dp:users> <dp:name>Snmp_User1</dp:name> <dp:name>Snmp_User2</dp:name> <dp:name>Snmp_User3</dp:name> </dp:users> </dp:ListUserReply></pre>
Response Header	<p>Return 200 OK.</p> <p>Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0</p>
Response Code	<p>400- Bad request. If the request body is invalid.</p> <p>400- API error. If the object either does not exist or is stale.</p> <p>403- Authorization Failure (for example, the user is not authenticated in the web session).</p> <p>500- Internal Server Error. This error is displayed for all generic server-side errors. Details about the error is given in the error notification that is displayed in the response body.</p> <p>503 Service Unavailable. When the request processing threshold is reached.</p>
Security Constraints	Only a Serviceability administrator can perform this operation.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
name	Represents the user string name.	String	Length <= 40	Yes	Alphanumeric	Alphanumeric dot, underscore, and hyphens are allowed. Space is not allowed.

Update

This implementation of user string updates the properties of the SNMP user string.

Only full update of SNMP v3 User API is allowed. Therefore, all the XML tags with valid values must be included while sending the update request. For more information, see [Update Implementation for SNMP/Syslog REST APIs, on page 239](#).

Table 61: Parameters of SNMP User String Update

URL	<code>https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/user</code>
HTTP Method	PUT
Input/Output Format	XML
Request	The PUT operation on the service endpoint updates the properties of the SNMP community. <code>PUT https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/user</code>
Content-type	Application/XML
Accept	Application/XML
Request Data Structure	<pre><?xml version="1.0" encoding="UTF-8" standalone="yes"?> <user> <name>Snm_User</name> <accessprivilege>ReadOnly</accessprivilege> <hosts> <host>192.0.2.0</host> </hosts> <authInfoReqd>true</authInfoReqd> <authProtocol>MD5</authProtocol> <authPassword>user@123</authPassword> <privacyInfoReqd>true</privacyInfoReqd> <privacyProtocol>AES-192</privacyProtocol> <privacyPassword>user@123456</privacyPassword> </user></pre>
Response Header	Return 200 OK. Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0

Response Code	<p>400- Bad request. If the request body is invalid.</p> <p>400- API error. If the object either does not exist or is stale.</p> <p>403- Authorization Failure (for example, the user is not authenticated in the web session).</p> <p>500- Internal Server Error (for example, the connection is broken with the database server or ORM or any other component).</p> <p>503 Service Unavailable. When the request processing threshold is reached.</p>
Security Constraints	Only a Serviceability administrator can perform this operation.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
name	Represents the user string name.	String	Length <= 40	Yes	Alphanumeric	Alphanumeric dot, underscore, and hyphens are allowed. Space is not allowed.
accessprivilege	Represents the access privileges of the user string.	String	-	Yes	ReadOnly (default), ReadWrite	Only ReadOnly or ReadWrite; Not case sensitive.
hosts	Represents a list of "host" tags.	-	-	Yes	If this tag is specified, then the host tag is mandatory.	-
host	Represents the management station host IP address. If the management station host IP address is not provided, then any host can request for the management information.	String	Valid IP address; number of host tags must be <= 255	Yes	A valid ip4 address	-
authInfoReqd	Authentication information is required.	Boolean	-	Yes	false, true	Case sensitive.
authProtocol	Authentication protocol.	String	-	No. If authInfoReqd is true, then this field is mandatory.	MD5 SHA-1	Value for this tag is set only when authInfoReqd is true.
authPassword	Authentication password.	String	-	No. If authInfoReqd is true, then this field is mandatory.	Alphanumeric with any special character.	Value for this tag is set only when authInfoReqd is true.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
privacyInfoReqd	Privacy information is required.	Boolean	-	Yes	false, true	Case sensitive. If privacyInfoReqd is true, then authInfoReqd must be set to true.
privacyProtocol	Privacy protocol.	String	-	No. If privacyInfoReqd is true, then this field is mandatory.	3DES AES-192 AES-256	Value for this tag is set only when privacyInfoReqd is true.
privacyPassword	Privacy password.	String	-	No. If privacyInfoReqd is true, then this field is mandatory.	Alphanumeric with any special character.	Value for this tag is set only when privacyInfoReqd is true.

Traps

Traps are messages alerting the SNMP manager to a condition on the network. Notifications can indicate various significant events such as:

- improper user authentication
- restarts
- the closing of a connection
- loss of connection to a neighboring router

and so on.

Create

This implementation of SNMP Trap string creates trap as mentioned in the request.

Table 62: Parameters of SNMP Trap string Post

URL	https:// <server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/trap
HTTP Method	POST
Input/Output Format	XML
Request	The POST operation on the service endpoint creates an SNMP Trap. POST https:// <server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/trap
Content-type	Application/XML
Accept	Application/XML

Request Data Structure	<pre><?xml version="1.0" encoding="UTF-8" standalone="yes"?> <trap> <name>trap1</name> <snmpversion>v2c</snmpversion> <communityOrUserRef>comm2</communityOrUserRef> <destinations> <destination> <ipAddr>192.0.2.0</ipAddr> <port>9999</port> </destination> </destinations> </trap></pre>
Response Header	<p>Return 201 CREATED.</p> <p>Response headers: HTTP/1.1 201 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0</p>
Response Code	<p>400- Bad request. If the request body is invalid.</p> <p>400- API error . If the object either does not exist or is stale.</p> <p>403- Authorization Failure (for example, the user is not authenticated in the web session).</p> <p>500- Internal Server Error. This error is displayed for all generic server-side errors. Details about the error is given in the error notification that is displayed in the response body.</p> <p>503 Service Unavailable. When the request processing threshold is reached.</p>
Security Constraints	Only a Serviceability administrator can perform this operation.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
name	Represents the trap string name.	String	Length <= 41	Yes	Alphanumeric	Alphanumeric dot, underscore, and hyphens are allowed; Space is not allowed.
snmpversion	Represents the SNMP version.	String	-	Yes	V1, V2C, V3	V1, V2C, V3
communityOrUserRef	Represents a community or user for which this trap is configured.	String	Length <= 41	Yes	Alphanumeric	Alphanumeric dot, underscore, and hyphens are allowed; Space is not allowed.
destinations	Represents the list of destination tag.	-	-	Yes	-	-
destination	Each destination tag has a mandatory ipAddr and port tag.	-	Number of destination tags must be <= 255	Yes	-	-

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
ipAddr	Represents the destination IP where traps have to be sent.	String	Valid IP address	Yes	Valid IP address	-
port	Represents the port on the destination where the traps have to be sent.	String	Length <= 5	Yes	The default value 162 is assumed when: - no value is specified - the value specified is 0	Numeric.

Delete

This implementation of SNMP Trap string deletes the traps from the listed traps.

Table 63: Parameters of SNMP Trap string Delete

URL	https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/trap/Name/<name>
HTTP Method	DELETE
Input/Output Format	XML
Request	The DELETE operation on the service endpoint deletes the properties of the Traps API. DELETE https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/trap/Name/<name>
Content-type	Application/XML
Accept	Application/XML
Response Header	Return 200 OK. Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0
Response Code	400- Bad request. If the request body is invalid. 400- API error . If the object either does not exist or is stale. 403- Authorization Failure (for example, the user is not authenticated in the web session). 500- Internal Server Error. This error is displayed for all generic server-side errors. Details about the error is given in the error notification that is displayed in the response body. 503 Service Unavailable. When the request processing threshold is reached.
Security Constraints	Only a Serviceability administrator can perform this operation.

Get

This implementation of SNMP Trap string retrieves the details of the trap.

Table 64: Parameters of SNMP Trap string Get

URL	https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/trap/Name/<name>
HTTP Method	GET
Input/Output Format	XML
Request	The GET operation on the service endpoint retrieves the details of the Trap API. GET https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/trap/Name/<name>
Content-type	Application/XML
Accept	Application/XML
Response Data Structure	<pre><dp:TrapReply ReturnCode="0"> <dp:Schema Version="1.0"/> <dp:trap> <dp:name>trap1</dp:name> <dp:snmpversion>V2C</dp:snmpversion> <dp:communityOrUserRef>comm2</dp:communityOrUserRef> <dp:destinations> <dp:destination> <dp:ipAddr>192.0.2.0</dp:ipAddr> <dp:port>9999</dp:port> </dp:destination> </dp:destinations> </dp:trap> </dp:TrapReply></pre>
Response Header	Return 200 OK. Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0
Response Code	400- Bad request. If the request body is invalid. 400- API error. If the object either does not exist or is stale. 403- Authorization Failure (for example, the user is not authenticated in the web session). 500- Internal Server Error. This error is displayed for all generic server-side errors. Details about the error is given in the error notification that is displayed in the response body. 503 Service Unavailable. When the request processing threshold is reached.
Security Constraints	Only a Serviceability administrator can perform this operation.

List

This implementation of SNMP trap string lists all the traps that are configured on the system.

Table 65: Parameters of SNMP Trap string Get

URL	https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/trap
HTTP Method	GET
Input/Output Format	XML
Request	The GET operation on the service endpoint lists all the traps that are configured on the system. GET https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/trap
Content-type	Application/XML
Accept	Application/XML
Response Data Structure	<pre><dp:TrapReply ReturnCode="0"> <dp:Schema Version="1.0"/> <dp:traps> <dp:trap> <dp:name>trap1</dp:name> </dp:trap> <dp:trap> <dp:name>trap2</dp:name> </dp:trap> </dp:traps> </dp:TrapReply></pre>
Response Header	Return 200 OK. Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0
Response Code	400- Bad request. If the request body is invalid. 400- API error. If the object either does not exist or is stale. 403- Authorization Failure (for example, the user is not authenticated in the web session). 500- Internal Server Error. This error is displayed for all generic server-side errors. Details about the error is given in the error notification that is displayed in the response body. 503 Service Unavailable. When the request processing threshold is reached.
Security Constraints	Only a Serviceability administrator can perform this operation.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
name	Represents the trap string name.	String	Length <= 41	Yes	Alphanumeric	Alphanumeric dot, underscore, and hyphens are allowed.

Update

This implementation of trap string updates the properties of the SNMP trap that is mentioned in the request.

Only full update of SNMP Traps API is allowed. Therefore, all the XML tags with valid values must be present while sending the update request. For more information, see [Update Implementation for SNMP/Syslog REST APIs, on page 239](#).

Table 66: Parameters of SNMP Trap string Put

URL	https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/trap
HTTP Method	PUT
Input/Output Format	XML
Request	The PUT operation on the service endpoint updates the properties of the SNMP trap that is mentioned in the request. PUT https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/trap
Content-type	Application/XML
Accept	Application/XML
Request Data Structure	<pre><?xml version="1.0" encoding="UTF-8" standalone="yes"?> <trap> <name>trap1</name> <snmpversion>v2c</snmpversion> <communityOrUserRef>comm2</communityOrUserRef> <destinations> <destination> <ipAddr>192.0.2.0</ipAddr> <port>9999</port> </destination> </destinations> </trap></pre>
Response Header	Return 200 OK. Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0
Response Code	400- Bad request. If the request body is invalid. 400- API error. If the object either does not exist or is stale. 403- Authorization Failure (for example, the user is not authenticated in the web session). 500- Internal Server Error. This error is displayed for all generic server-side errors. Details about the error is given in the error notification that is displayed in the response body. 503 Service Unavailable. When the request processing threshold is reached.
Security Constraints	Only a Serviceability administrator can perform this operation.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
name	Represents the trap string name.	String	Length <= 41	Yes	Alphanumeric	Alphanumeric dot, underscore, and hyphens are allowed.
snmpversion	Represents the SNMP version.	String	-	Yes	V1, V2C, V3	V1, V2C, V3
communityOrUserRef	Represents a community or user for which this trap is configured.	String	Length <= 41	Yes	Alphanumeric	Alphanumeric dot, underscore, and hyphens are allowed.
destinations	Represents the list of destination tag.	-	-	Yes	-	-
destination	Each destination tag has a mandatory ipAddr and port tag.	-	Number of destination tags must be <= 255	Yes	-	-
ipAddr	Represents the destination IP where traps have to be sent.	String	Valid IP address	Yes	Valid IP address	-
port	Represents the port on the destination where the traps have to be sent.	String	Length <= 5	Yes	The default value 162 is assumed when: - no value is specified - the value specified is 0	Numeric.

Syslog

Syslog is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in collection of logs and alerts. Cisco devices can send their log messages to a Unix-style SYSLOG service. A SYSLOG service simply accepts messages, and stores them in files or prints them according to a simple configuration file.

For a Syslog instance, there can a maximum of five Syslog collector destinations that you can configure to receive the Syslog messages simultaneously.

Update

This implementation of syslog updates syslog parameters that are mentioned in the request.

Only full update of Syslog API is allowed. Therefore, all the XML tags with valid values must be present while sending the update request. For more information, see [Update Implementation for SNMP/Syslog REST APIs, on page 239](#).

Table 67: Parameters of syslog API String Create

URL	https://<server>:<port>/icm-dp/rest/DiagnosticPortal/syslog
HTTP Method	PUT
Input/Output Format	XML
Request	The PUT operation on the service endpoint updates the details of the SNMP REST syslog API. PUT https://<server>:<port>/icm-dp/rest/DiagnosticPortal/syslog
Content-type	Application/XML
Accept	Application/XML
Request Data Structure	<pre><?xml version="1.0" encoding="utf-8"?> <syslogParameters> <syslogInstanceName >inst1</syslogInstanceName > <loggerNode>LoggerA</loggerNode> <enableFeed>true</enableFeed> <collectorAddressList> <collectorAddress> <address>192.0.2.1</address> <port>514</port> </collectorAddress> <collectorAddress> <address>192.0.2.1</address> <port>515</port> </collectorAddress> </collectorAddressList> <disablePing>true</disablePing> </syslogParameters></pre>
Response Header	Return 200 OK. Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0
Response Code	400- Bad request. If the request body is invalid. 400- API error . If the object either does not exist or is stale. 403- Authorization Failure (for example, the user is not authenticated in the web session). 500- Internal Server Error. This error is displayed for all generic server side errors. Details about the error will be given in the error notification that is displayed in the response body. 503 Service Unavailable. When the request processing threshold is reached.
Security Constraints	Only a Serviceability administrator can perform this operation.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
syslogInstanceName	Represents the name of the logger instance.	String	Length <= 32	Yes	Alphanumeric	Only valid instance configured in the logger machine.

Tag	Description	Data Type	Input Constraints	Required Fields	Possible Value	Additional Validation
loggerNode	Represents the logger node.	String	-	Yes	LoggerA or LoggerB	Only LoggerA or LoggerB; Not case sensitive
enableFeed	If set to true, sends the syslog messages to the configured syslog collector. Also, any modification to the collector address and other parameters requires setting enableFeed to true.	Boolean	-	Yes	-	true/false; case sensitive.
collectorAddressList	Represents a list of collectorAddress.	-	-	Yes	-	-
collectorAddress	Each collectorAddress tag should have a mandatory address and port tag.	-	Number of collectorAddress tags must be <= 5	Yes	-	-
address	Represents the Syslog collector IP address or host name.	String	Host or IP address	Yes	Alphanumeric	A valid host name or IP address.
port	Port on the syslog collector destination.	String	Value should be <= 65535	Yes	Only numeric	514 (default). If value is specified as 0, then the default value is assumed.
disablePing	If set to true, disables ping messages to the syslog collector destination.	Boolean	-	Yes	-	true/false; case sensitive.

List

This implementation of syslog lists all the instances that are configured on the system.

Table 68: Parameters of Syslog API String List

URL	https://<server>:<port>/icm-dp/rest/DiagnosticPortal/syslog
HTTP Method	GET
Input/Output Format	XML
Request	The GET operation on the service endpoint lists the instances of the SNMP REST syslog API that are configured on the system. GET https://<server>:<port>/icm-dp/rest/DiagnosticPortal/syslog
Content-type	Application/XML
Accept	Application/XML

Response Data Structure	<pre><dp:ListLoggerInstancesReply ReturnCode="0"> <dp:Schema Version="1.0"/> <dp:LoggerInstances> <dp:LoggerInstance> <dp:loggerInstanceName >inst1</dp:loggerInstanceName > <dp:loggerNode>LoggerA</dp:loggerNode> </dp:LoggerInstance> </dp:LoggerInstances> </dp:ListLoggerInstancesReply></pre>
Response Header	<p>Return 200 OK.</p> <p>Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0</p>
Response Code	<p>400- Bad request. If the request body is invalid.</p> <p>400- API error . If the object either does not exist or is stale.</p> <p>403- Authorization Failure (for example, the user is not authenticated in the web session).</p> <p>500- Internal Server Error. This error is displayed for all generic server side errors. Details about the error will be given in the error notification that is displayed in the response body.</p> <p>503 Service Unavailable. When the request processing threshold is reached.</p>
Security Constraints	Only a Serviceability administrator can perform this operation.

Get

This implementation of syslog retrieves the details of the syslog parameters for a logger instance.

Table 69: Parameters of Syslog API String

URL	https://<server>:<port>/icm-dp/rest/DiagnosticPortal/ syslog/syslogInstanceName /<name>&loggerNode/<node>
HTTP Method	GET
Input/Output Format	XML
Request	<p>The GET operation on the service endpoint retrieves the details of the syslog parameters for a logger instance.</p> <p>GET https://<server>:<port>/icm-dp/rest/DiagnosticPortal/syslog/syslogInstanceName /<name>&loggerNode/<node></p>
Content-type	Application/XML
Accept	Application/XML

Response Data Structure	<pre><dp:syslogReply ReturnCode="0"> <dp:Schema Version="1.0"/> <dp:syslogParameters> <dp:syslogInstanceName>test1</dp:syslogInstanceName> <dp:loggerNode>LoggerA</dp:loggerNode> <dp:enableFeed>false</dp:enableFeed> <dp:collectorAddressList> <dp:collectorAddress> <dp:address>192.1.2.1</dp:address> <dp:port>514</dp:port> </dp:collectorAddress> </dp:collectorAddressList> <dp:disablePing>false</dp:disablePing> </dp:syslogParameters> </dp:syslogReply></pre>
Response Header	<p>Return 200 OK.</p> <p>Response headers: HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: application/xml Server: Microsoft-HTTPAPI/2.0</p>
Response Code	<p>400- Bad request. If the request body is invalid.</p> <p>400- API error . If the object either does not exist or is stale.</p> <p>403- Authorization Failure (for example, the user is not authenticated in the web session).</p> <p>500- Internal Server Error. This error is displayed for all generic server side errors. Details about the error will be given in the error notification that is displayed in the response body.</p> <p>503 Service Unavailable. When the request processing threshold is reached.</p>
Security Constraints	Only a Serviceability administrator can perform this operation.

Update Implementation for SNMP/Syslog REST APIs

Only full update of Community, User, Traps, and Syslog APIs is allowed. The following example demonstrates how to send an update request for the Community, User, Traps, and Syslog APIs.

Consider that a community is added with the following properties:

```
POST https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/community
<?xml version="1.0" encoding="utf-8"?>
<community>
  <name>Public_Community</name>
  <snmpversion>V1</snmpversion>
  <accessprivilege>ReadOnly</accessprivilege>
  <hosts>
    <host>192.0.2.0</host>
    <host>192.0.2.1</host>
  </hosts>
</community>
```

If you want update one of the hosts from **192.0.2.0** to **192.0.2.250**, the XML body of the update request must contain the following properties:

```
PUT https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/community
<?xml version="1.0" encoding="utf-8"?>
<community>
  <name>Public_Community</name>
```

```

<snmpversion>V1</snmpversion>
<accessprivilege>ReadOnly</accessprivilege>
<hosts>
  <host>192.0.2.250</host>           //modified IP
  <host>192.0.2.1</host>           //existing IP retained
</hosts>
</community>

```

Diagnostic Framework Troubleshooting

The Diagnostic Framework is self contained and does not require any additional configuration other than assigning users. If you encounter any issues with the service, see the following table:

Table 70: Diagnostic Framework Troubleshooting

Issue	Troubleshooting / Remedy
Diagnostic Framework service does not start	<p>Check if required service HTTP SSL (and IIS, when installed) is started without any errors. Check Windows Event log for errors and resolve any issues with the required services.</p> <p>Make sure none of the configuration files is missing.</p> <p>Check Event Viewer and Diagnostic Framework log file for any initialization errors.</p>
Cannot access any API from the supported browser client	<p>Confirm that you are using a supported browser by checking the <i>Contact Center Enterprise Compatibility Matrix</i> at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.</p> <p>Confirm the base URL is correct; compare it with the URL in the service configuration file DiagFwSvc.exe.config.</p> <p>Confirm the API used is valid.</p> <p>Make sure the API is accessed using HTTPS.</p> <p>Make sure the credentials used as valid, check Windows Event log for any authentication errors and Diagnostic Framework log for any authorization errors.</p> <p>Use DiagFwCertMgr utility to validate the certificate binding to the port in use. Recreate or rebind the certificate if any issues were found.</p> <p>Clear the supported browser cache and restart the browser.</p> <p>Verify that the Windows Firewall is either turned off, or that it was configured with the ICM Security Wizard, which ensures that a proper exception is in place for the Diagnostic Framework to work.</p>
Some commands work, and others do not seem to work.	<p>Confirm that you are using a supported browser by checking the <i>Contact Center Enterprise Compatibility Matrix</i> at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.</p>

DUMPLOG

The DUMPLOG utility converts binary log files written by Unified ICM/Unified CCE processes into readable text format. DUMPLOG can optionally display the binary log files in Cisco Log message format. For more information about the Cisco Log format, see [The Cisco Log Message Format, on page 63](#). For more information about this utility, see the *How to Use the DumpLog Utility Tech Note* at https://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_tech_notes_list.html.

Header

Cisco Log formatted log entries include a more comprehensive header compared to DUMPLOG standard format.

DumpLog Standard Format

Standard formatted DUMPLOG entries display the following fields:

```
<TIMESTAMP> <COMPONENT-PROCESS> <MESSAGE>
```

The timestamp is represented as a 24-hour value (hh:mm:ss). It does not include the date, which appears on a separate line at the beginning of the file and when a new day starts. For example:

```
Events from February 8, 2007
00:37:44 ra-rtr MDS is in service.
```

Cisco Log Format

Cisco Log formatted DUMPLOG entries display the following fields:

```
<SEQNUM>: <HOST>: <TIMESTAMP> <TIMEZONE>: %APPNAME: %<TAGS>:<MESSAGE>
```

Example DUMPLOG message

Below is an example of a Cisco Log formatted DUMPLOG message. An actual log entry appears on a single line.

```
10: CICMRGRA: Feb 8 2007 05:37:44.658 +0000: %ICM_Router_ProcessSynchronization:
[comp=Router-A]
[pname=rtr][iid=acme][sev=info]: MDS is in service.
```

Usage

You can use the following command-line options for the **dumplog** utility to view the log files within a specific time period. You can define the time period with the /bd, /bt, /ed, and /et switches.

```
dumplog[ProcessName(s)][/dir Dirs] [/if InputFile] [/o] [/of OutputFile] [/c] [/bd BeginDate(mm/dd/yyyy)]
[/bt BeginTime(hh:mm:ss)] [/ed EndDate(mm/dd/yyyy)] [/et EndTime(hh:mm:ss)] [/hr HoursBack] [/all]
[/last] [/prev] [bin] [/m MatchString] [/x ExcludeString] [/ms] [/debug] [/ciscoLog] [/unzipCmdPrefix Prefix
for Unzip command] [/unzipCmdInfix Infix for Unzip command] [/unzipCmdPostfix Postfix for Unzip command]
[/unzipTempfile Temporary filename for unzip command] [/zipPostfix Postfix of zipped files] [/tzadjustoff]
[/help] [?]
```

Parameter	Description
ProcessName(s)	This command dumps the current day log for this process, unless you specify different dates or times with other arguments.
[/dir Dirs]	This command specifies the directory location of the log files for any processes listed on the command line after the /dir switch. If no /dir switch is used, the current directory is used by default.
[/if]	The InputFile specifies a specific .ems file to dump. The /if token is optional. If you specify an input file, the /bd, /bt, /ed, /et, /hr, and /all arguments are ignored.
/o	Writes output to a text file in the \logfiles directory. The filename is formed when you add the .txt suffix to the specified process prefix or input file name (without the .ems suffix). The file is written to the current directory.
/of	OutputFile specifies an output text file; for example, c:\temp\mylog.txt.
/c	Specifies continuous output. The command does not exit after it reaches the end of the log. Instead, it waits and writes any further entries that appear in the log.
/bd	BeginDate(mm/dd/yyyy) specifies the begin date. If used with /bt, this specifies a range of dates. Otherwise, dumplog dumps events for only the specified date.
/bt	BeginTime(hh:mm:ss) specifies the begin time. Use with /et in order to specify a range of time.
/ed	EndDate(mm/dd/yyyy) specifies the end date. Use with /bd in order to specify a range of days.
/et	EndTime(hh:mm:ss) specifies the end time. Use with /bt in order to specify a range of time.
/hr	HoursBack specifies a number of hours back from the current time.
/all	Displays all information from the specified process log files.
/last	Displays information from the most recent log file for the process.
/prev	Displays information from the next to last log file for the process.
/m	MatchString displays only events that contain a match for the specified string.
/x	ExcludeString displays only events that do not contain a match for the specified string.
[/ms]	Displays milliseconds in time stamps.
[/mc]	Use multiple colors when you dump merged logs. Each process is given a different color. You must specify either a ProcessPrefix or an InputFile. If you give only a ProcessPrefix value (for example, rtr, nm, or lgr), dumplog displays the current day log for that process by default.
/ciscoLog	Enables the CiscoLog functionality.
/unzipCmdPrefix	Prefix parameters for unzip, for example gzip -d -c.

Parameter	Description
<code>/unzipCmdInfix</code>	Infix parameter for unzip, for example ">".
<code>/unzipCmdPostfix</code>	Postfix parameter for unzip, for example "".
<code>/unzipTempfile</code>	Temp file for unzip, for example "temp.ems".
<code>/zipPostfix</code>	File postfix parameter, for example ".gz".
<code>/tzadjustoff</code>	<p>When the EMS files are copied to a system in a different timezone, or if the timezone on the system is changed, without this option, all the queries made will be relative to the machine on which the logfiles were generated. Otherwise, /tzadjustoff is used in order to switch the behavior where queries are made with respect to this machine time.</p> <p>Note Use /tzadjustoff if you are gathering logs across a DaylightSavingsTime (DST) change.</p>



Note The contents of the APPNAME and TAGS fields differ from those previously described in section 5.1.

Table 71: APPNAME and TAGS Used in DUMPLOG Trace Output

Field	Description
APPNAME	PRODUCT_COMPONENT_MESSAGECATEGORY PRODUCT - always ICM COMPONENT – such as Router MESSAGECATEGORY – such as ProcessSynchronization
TAGS	Acceptable tags are: [comp=%s] - component name including side, such as Router A [pname=%s] - process name, such as rtr [iid=%s] - instance name, such as acme [sev=%s] – severity, such as info and optionally [part=%1.%2/%3], which is used only for multi-line entries as described later in this section.

Timestamp

The timestamp displayed in DUMPLOG standard format is in local time relative to the server on which DUMPLOG is run. The timestamp displayed in Cisco Log format is in GMT time independent of the server on which DUMPLOG is run.



Note Date/time options specified on the command line are entered in local time, regardless of whether the Cisco Log option is selected. Therefore, timestamps displayed as part of the Cisco Log formatted entry might appear to be outside of the date/time range selected.

Multi-line Entries

The message portion of some DUMPLOG entries might contain one or more embedded new line characters (`\n`), which cause the messages to appear on multiple lines and might also include blank lines. This is especially true for entries that contain statistics.

For a DUMPLOG standard formatted message, only the first line contains the header field as shown in the following example:

```
00:36:09 ra-nm ICM\acme\RouterA node reporting process statistics for process ccag.
    Process name: ccag
    Process status: A
    Process ID: 6c0
    Number of times process started: 1
    Last start time: 00:35:31 2/8/2007
    Pings completed in zero time: 0
    Pings completed in first third: 0
    Total first third milliseconds: 0
    Pings completed in second third: 0
    Total second third milliseconds: 0
    Pings completed in third third: 0
    Total third third milliseconds: 0
    Longest Ping time: 0
```

For a Cisco Log formatted message, each line contains a separate header. In the example below, however, each entry spans several lines due to page size constraints.

```
19: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.1/14]: ICM\acme\RouterA node reporting process statistics for process
ccag.
20: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.2/14]: Process name: ccag
21: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.3/14]: Process status ACTIVE
22: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.4/14]: Process ID 6c0
23: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.5/14]: Number of times process started 1
24: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.6/14]: Last start time: 00:35:31 2/8/2007
25: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.7/14]: Pings completed in zero time: 0
26: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.8/14]: Pings completed in first third: 0
27: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.9/14]: Total first third milliseconds: 0
28: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.10/14]: Pings completed in second third: 0
29: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.11/14]: Total second third milliseconds: 0
30: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.12/14]: Pings completed in third third: 0
```

```

31: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.13/14]: Total third third milliseconds: 0
32: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown:
[comp=Router-A][pname=nm][iid=acme]
[sev=info][part=19.14/14]: Longest Ping Time: 0

```

To differentiate each line in the entry, the part tag is added to each header:

```
[part=#1.#2/#3]
```

Where:

#1 = the sequence number of the first line (this is the same for all lines in the entry)

#2 = the part number of the specific line

#3 = the total number of parts in the entry

Note the line beginning with sequence number 32, where `[part=19.14/14]`:

#1 = 19. #2 = 14 / #3 = 14



Note The log files are zipped according to the parameters specified in the EMS registry settings. While dumping the logs, if one log file transitions to the next log file very quickly, then do one of the following to avoid an error:

- Provide an EndTime (/et) with BeginTime (/bt)
- Increase the file size per log



Note Collecting logs on the UCCE system using dumplog utility impacts CPU and disk utilization. Running dumplog simultaneously on multiple VMs sharing the same disk can cause problems for the disk during peak busy hour if system resources are being stretched near the system limits for BHCA.

For information about system limits for busy hour call attempts (BHCA), see Solution Design Guide for Cisco Unified Contact Center Enterprise at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html>.

Some possible workaround include:

- Saving off EMS zip files, and dumping them on an idle system.
 - Using System CLI which runs at a lower system priority.
 - Serialize dumplog log collection by taking the logs that are likely to wrap first.
-

EMSMON

While title bar status information is available in the Diagnostic Portico, real time messages can be viewed using EMSMON.

EMSMON displays process messages as they are logged. It displays the same content as the former process windows, except for the title bar and the stdout and stderr output. Logged events for the selected processes appear in the EMSMON window. However, rare error condition messages (for example, shelled processes) that go to stdout do not appear in an EMSMON window.

To change the number of lines each EMSMON window retains, modify the command window parameters.

You can cut and paste in EMSMON (just as in the command windows). It is safer to cut and paste in EMSMON.

For history (events before EMSMON starting), use DUMPLOG.

How to Run EMSMON

You can start EMSMON at anytime, even when the process is not running. (You can have a batch file on a machine to start sessions.) If the process is down, EMSMON displays messages from the process when the process starts. EMSMON does not end when the process ends. To end EMSMON, press **Ctrl+C** or close the window.

EMSMON has the same parameters as ProcMon:

```
<instance> <node> <process> [<process>...] [<system>] [<LanguageID>]
```

The system parameter is optional. Use the system parameter to remotely run EMSMON.

For example, if the instance node is “ucce”, to monitor the JTAPI gateway on PG1A, type the following:

```
EMSMON ucce PG1A jgw1
```

If you are remote (on another PG) and the system name is UCCEPG1A, type:

```
EMSMON ucce PG1A jgw1 UCCEPG1A
```



Note A trust relationship must exist between the two machines. (Use the “NET USE” command or complete an operation that sets up a trust [for example, map a drive].)

The language identification parameter is also optional. As logging is only supported in the English language, it needs to be set to "1033" (for English) whenever the OS is running any other language.

Monitoring Process

Use one EMSMON only for each process.

Run EMSMON Remotely

To reserve system resources for Unified CCE processes, EMSMON can be run from any CCE core system to remotely monitor processes on another CCE system, preferably from an less critical component like a Client Admin Workstation.

EMSMON Connections

You can have one local connection and five remote connections per process. When the number of connections is exceeded, the oldest session is disconnected with the message “You are being disconnected because another user has connected to this named pipe.”

Running EMSMON against a process that is under heavy load is not supported, and can lead to instability in the target process. If your system is running a heavy call load, your EMSMON connections may disconnect and the message “You are being disconnected because the system is running a heavy call load; this connection may impact the performance of the system. Ensure not to reconnect your EMSMON sessions until your system returns to a normal call load.” appear.



Note To prevent Unified CCE processes from exceeding the system memory, Unified CC processes may stop sending queued event messages to slow or paused EMSMON clients. If this occurs, EMSMON clients display a message indicating one of the clients fell behind and there is a gap. This message is also logged in the processes event log. This can happen if a particular EMSMON client is too slow or paused by quick edit or Ctrl+S for example. This does not affect the Unified CCE process, only the EMSMON client.

Unified CCE Certificate Monitoring Service

The Unified CCE Certificate Monitor is a service that monitors the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) based certificates and keys. These certificates and keys are primarily used by the Unified CCE components at the node level. It alerts the system administrator about the validity and expiry of these certificates through Event Viewer. The events from the Unified CCE Certificate Monitoring service are displayed under **Windows Logs > Application**.

This service helps the system administrator to ensure that the systems are installed with valid security certificates without interrupting the Unified CCE services that are running.

Service Installation

Unified CCE Certificate Monitor is installed as a Windows service during ICM installation. Unified CCE Certificate Monitor is not controlled using the Diagnostic Framework Portico. You can view, start, stop, or restart the service from Windows Task Manager.

Certificate Monitoring Events

The Unified CCE Certificate Monitor validates the certificates and keys and reports any error or warning messages to the Event Viewer. The Event Viewer displays the following events:

Table 72: Certificate Monitor Events

Event Type	Event ID	Source	Category
Error	1	CISCO SYSTEMS, INC.ICM	Certificate Monitor
Warning	2	CISCO SYSTEMS, INC.ICM	Certificate Monitor

Certificate and Key Validation

The Unified CCE Certificate Monitor performs the following validations to confirm that a certificate or a key is valid. In case of any discrepancies, the service displays the corresponding error or warning message.

Validation	Description	Error or Warning
Certificate or Key Validation	<p>The certificate and key is validated for:</p> <ul style="list-style-type: none"> • Existence • Format Type • Integrity <p>Note PEM is the only supported certificate format.</p>	<p>Error:</p> <p>Case 1: When the certificate is not available in the path: Certificate <certpath> not found.</p> <p>Case 2: When the key is not available in the path: Private key not found.</p> <p>Case 3: When the certificate has an incorrect format: Failed to load the Security certificate.</p> <p>Case 4: When the key has an incorrect format: Failed to load the private key. Key format is not supported.</p> <p>Case 5: When the key and certificate are not matching: Certificate <certpath> is not matching with the private key.</p>
Subject Validation	The Common Name (CN) is validated for the hostname and domain.	<p>Error:</p> <p>Case 1: When the hostname does not match with the certificate: Host name is not matching with Certificate.</p>
Timestamp Validation	Validates the "Not Before" and "Not After" attributes of the timestamp to confirm the certificate or key validation period.	<p>Warning:</p> <p>Case 1: When the certificate is not valid before the timestamp: Certificate <certpath> is not valid before the timestamp.</p> <p>Case 2: When the certificate is not valid after the timestamp: Certificate <certpath> will expire on <timestamp>.</p>
Issuer Validation	Checks if the certificate is a self-signed certificate. A registry value is used to enable or disable this check. By default, the self-signed certificate check is disabled.	<p>Warning:</p> <p>Case: When a self-signed certificate is used: Self-signed certificate is used.</p>
Chain Validation	<p>The certificate chain is validated end-to-end.</p> <p>Note The root and intermediate CA certificates must be present at the trusted certificates location on the system.</p>	<p>Error:</p> <p>Case: When a certificate in the chain is not found: Certificate chain validation failed. Error: <error message></p>

Serviceability

The Unified CCE Certificate Monitor uses EMS Framework to create and manage its trace files. The certificate monitoring trace files are created in the folder: <ICM_Drive>:\icm\certmon\logfiles. You can use the DUMPLOG utility to extract trace files.

Procedure

-
- Step 1** To extract trace files, open command prompt and navigate to the `logfiles` folder.
- Step 2** Run the command `C:\icm\certmon\logfiles>dumplog ciscocertmon /<last>/<o>`. In this example, trace files since the last restart are generated.
-

Supported Log Levels

Unified CCE Certificate Monitor supports four levels of trace configuration based on the level of trace detail and performance impact.

By default, the trace level is set to the level "Error." To change the trace level settings, modify the registry `Software>Cisco System Inc\ICM\CertMon\LogLevel` with the appropriate level.

Trace Level	Description
Error	Has minimal or no performance impact. By default, the log level is set to Error.
Warning	Log more detailed (plus error level) trace messages, small performance impact.
Info	Log more detailed (plus warning or error level) trace messages, medium performance impact.
Debug	Log most detailed (plus error, warning, or info level) trace messages, high performance impact.

Configuration Parameters

For the Unified CCE Certificate Monitor service, the configuration parameters are controlled through the registry at `Software>Cisco System Inc\ICM\CertMon`.

You can configure the following parameters as required:

Configuration Parameter	Description
<code>PollingIntervalInMinutes</code>	The interval in minutes at which the system reports an error or warning.
<code>RejectSelfSignedCertificates</code>	If the value is set to a non-zero value, a warning message is displayed stating that the certificate is a self-signed certificate. This is applicable when the node is configured with a self-signed certificate for its Unified CCE secured operations.
<code>WarningFrequencyInHours</code>	Frequency in hours at which the system displays warning messages. The default value is 24 hours.

Configuration Parameter	Description
WarningThresholdInDays	Frequency in days at which the system displays a warning message for certificate expiry. The default value is 15 days.



CHAPTER 10

Serviceability for VOS-Based Contact Center Applications

- [VOS-Based Contact Center Applications, on page 251](#)
- [Real Time Monitoring Tool, on page 251](#)
- [Disaster Recovery, on page 260](#)

VOS-Based Contact Center Applications

This chapter describes serviceability for all Cisco Voice Operating System (VOS)-based Contact Center applications. VOS-based Contact Center applications include, for example, Live Data, Cisco Identity Service, Cisco Unified Intelligence Center and Cloud Connect.

Real Time Monitoring Tool

For Cisco Unified Intelligence Center, Live Data, and Cisco Identity Service (Cisco IdS), download the Real Time Monitoring Tool (RTMT) from the Cisco Unified Intelligence Center Administration page (**Tools > RTMT Plugin Download**).

Live Data and the Cisco IdS do not host the RTMT installer. For this reason, always connect to the Cisco Unified Intelligence Center Server and sign in to the Administration page to download the RTMT installer. You can, however, run the same RTMT client to connect to any of the Cisco Unified Intelligence Center, Live Data, or Cisco IdS servers (standalone or coresident).

RTMT runs as a client-side application. You can install RTMT on a Windows workstation or a Linux machine. RTMT is cluster-aware. RTMT provides critical service and performance monitoring (perfmon), trace/log collection and viewing, and Alert Management on the node for the IP address you request at launch. RTMT does not provide the status of all critical applications on all the nodes at the same time.

Use RTMT to:

- Monitor the health of the system by generating email alerts for objects whose values go above or below a threshold
- Collect and view traces
- View syslog messages

- Monitor performance counters

RTMT has extensive online help. Refer to it for information on alerts, schedule collection, performance monitoring, and collecting and downloading tracing and logging data.

Install and Launch RTMT

Procedure

-
- Step 1** Log in to your Cisco Unified Intelligence Center Administration page through your browser.
- Note** The Live Data and the Cisco IdS servers do not provide the RTMT download link.
- Note** For Cloud Connect, download and install RTMT on a client computer. Use the following URL <https://FQDN:8443/plugins/CcmServRtmtPlugin.exe>. Where, FQDN is the Fully Qualified Domain Name of the Cloud Connect Primary or Secondary Node.
- Step 2** Click **Tools > RTMT Plugin Download**.
- Step 3** On the download page:
- Select the **Windows** platform.
 - Click **Download**.
 - Locate the CuicServRtmtPlugin.exe file (where you downloaded it). Right-click the file, and choose **Properties**.
 - Click the **Compatibility** tab, and check the **Run this program in compatibility mode for** check box. From the drop-down list, choose applicable **Windows** version and click **OK**.
 - Run CuicServRtmtPlugin.exe, or save and then run it from the saved location.
 - Follow the prompts and click the buttons on the installation screens.
- Step 4** To launch:
- Click the **Cisco Unified Real-Time Monitoring Tool 11.5** desktop icon.
 - In the Host IP Address field, enter the IP address for the node you want to monitor.
 - Accept the default port (8443).
 - Check Secure Connection. You see an error if the Host IP Address is not found or there is no network connection.
 - Click **Yes** to accept the certificate.
 - Enter the User Name and Password for a superuser. (Only a superuser can install RTMT.)
 - If a message appears indicating that a time zone mismatch exists, click **No** to launch RTMT in your current time zone.
 - Click **OK** to accept the default configuration.
- Note** The performance counters are documented in the *Administration Console User Guide for Cisco Unified Intelligence Center*. The performance counters are not documented in the Online help.
-

RTMT Client Support Services

RTMT uses the following services/servlets:

- Cisco AMC service
- Cisco CallManager Serviceability RTMT
- Cisco RIS Data Collector
- Cisco Tomcat Stats Servlet
- Cisco Trace Collection Service
- Cisco Log Partition Monitoring Tool
- Cisco SOAP-Real_Time Service APIs
- Cisco-SOAP-Performance Monitoring APIs
- Cisco RTMT Reporter Servlet

The RTMT Interface

The following RTMT system monitoring objects are available in the left pane of the RTMT page:

- **System Summary**

Displays information on Virtual Memory usage, CPU usage, Common Partition usage, and the alert history log.

- **Server**

Server objects are:

- **CPU and Memory** - Displays information on Virtual memory usage and CPU usage for the server.
- **Process** - Displays information on the processes running on the server.
- **Disk Usage** - Displays information on the disk usage on the server.
- **Critical Services** - Displays the name of the critical service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services have existed in a particular state for the server or for a particular server in a cluster (if applicable).

The Cisco Unified Intelligence Center services are listed under the **Intelligence Center** tab. The Live Data and Cisco IdS services are listed, along with the System services, under the **System** tab.

- **Performance**

Performance objects are:

- **Performance** - Performance monitoring allows you to monitor performance counters related to the Unified Intelligence Center server. You can continuously monitor a set of preconfigured objects and receive notification in the form of an email message. You can associate counter threshold settings to alter notification. Up to six perfmon counters in one chart for performance comparisons can be displayed. Performance queries can be used to add a counter to monitor. You can also save and

restore settings, such as counters being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.

- **Performance Log Viewer** - Displays data for counters from perfmon CSV log files in a graphical format.

- **Tools**

Tools objects are:

- **Alert Central** - Displays the history and status of every alert in the system. Click the **Intelligence Center** tab to see Unified Intelligence Center alerts, including those related to Cisco IdS.
- **Trace & Log Central** - Allows you to browse or download trace and log files for a specific date range or absolute time.
- **Job Status** - Shows the status of trace collection events.
- **Syslog Viewer** - Allows you to view (by node) the system, application, and security logs.
- **VLT** - Not applicable.
- **AuditLog Viewer** - Allows you to view system audit logs.

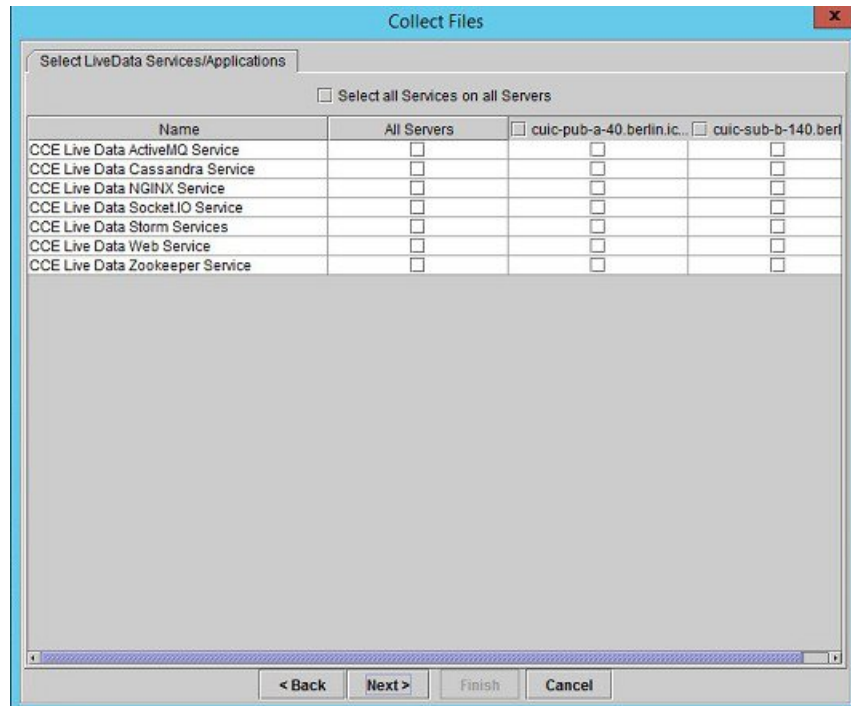
Download Trace and Log Files

Perform the following steps to download the trace and log files for Cisco Unified Intelligence Center, Live Data, Cisco IdS and Cloud Connect.

Procedure

- Step 1** Run RTMT to connect to the target server, then choose **Tools > Trace & Log Central** in the **System** pane.
- Step 2** Click **Collect Files**.
- Step 3** Click **Next** to browse through and select services and applications for which you want to collect files. For example, you can select one or more Live Data services; the list is shown here.

Figure 30: Select LiveData Services/Applications



- Step 4** When you finish selecting services and applications, you can choose either of the **Collection File Options**:
- **Absolute Range** - Choose the **Reference Server Time Zone** from the drop-down list. Then choose the **From Date/Time** and the **To Date/Time**.
 - **Relative Range** - From the drop-down lists, choose the number of files generated and the time duration (**Minutes, Hours, Days, Weeks, or Months**).
- Step 5** Choose the **Download File Options**:
- a. Choose either the **Active Partition** or **Inactive Partition** from the drop-down list.
 - b. Browse to or provide the path to the **Download File Directory**.
 - c. Select the **Zip Files** or **Do Not Zip Files** option.
 - d. To remove the log files from the server, check the **Delete Collected Log Files from Server** check box.
- Step 6** Click **Finish**.
-

View the Status of Services

Procedure

Run RTMT to connect to the target server, then choose **Server > Critical Services** in the **System** pane.

You see a number of services on the **System** tab, as shown in the following example.

Figure 31: RTMT Critical Services System Tab

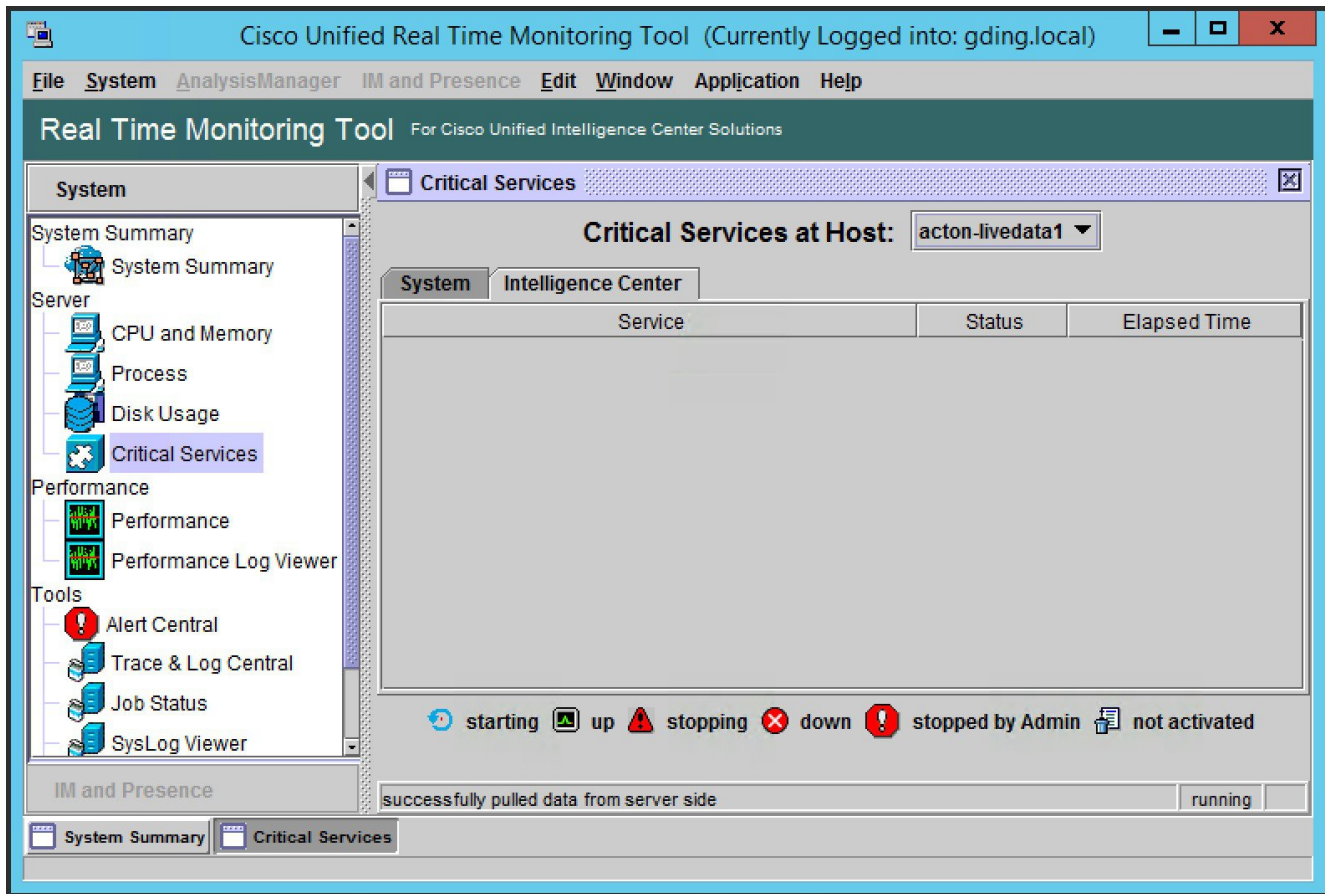
The screenshot shows the Real Time Monitoring Tool (RTMT) interface. The main window is titled "Real Time Monitoring Tool For Cisco Unified Intelligence Center Solutions". The "System" pane on the left is expanded to "Critical Services". The main area displays "Critical Services at Host: acton-livedata1". Below this, there is a table with columns for "Service", "Status", and "Elapsed Time". The table lists various services, all of which are currently "up". A legend at the bottom of the table defines the status icons: starting (blue arrow), up (green square), stopping (red triangle), down (red X), stopped by Admin (red circle with exclamation mark), not activated (blue square with white X), and Unknown Status (green square with white X). A status bar at the bottom indicates "successfully pulled data from server side" and "running".

Service	Status	Elapsed Time
A Cisco DB	up	1 Days 08:09:57
A Cisco DB Replicator	up	1 Days 09:28:44
Cisco AMC Service	up	1 Days 09:28:18
Cisco Audit Event Service	up	1 Days 09:28:17
Cisco CDP	up	1 Days 09:28:30
Cisco CDP Agent	up	1 Days 09:28:37
Cisco CallManager Serviceability	up	1 Days 09:16:59
Cisco CallManager Serviceability RTMT	up	1 Days 09:17:50
Cisco Certificate Change Notification	up	1 Days 09:28:23
Cisco Certificate Expiry Monitor	up	1 Days 09:28:24
Cisco DRF Local	up	1 Days 09:28:25
Cisco DRF Master	up	1 Days 09:28:26
Cisco Database Layer Monitor	up	1 Days 09:28:43
Cisco Log Partition Monitoring Tool	up	1 Days 09:28:31
Cisco RIS Data Collector	up	1 Days 09:28:19
Cisco RTMT Reporter Servlet	up	1 Days 09:17:50

Live Data and Cisco IdS services are also included on the **System** tab. To view the Unified Intelligence Center services, click the **Intelligence Center** tab.

When RTMT is connected to either a Unified Intelligence Center standalone server or a Cisco IdS standalone server, no services are listed on the Intelligence Center tab, as shown in the following figure.

Figure 32: RTMT Critical Services Intelligence Center Tab (Unified Intelligence Center or Cisco IdS Standalone)



When RTMT is connected to standalone cloud connect server. **Cloud Connect** services will be included as part of the **System** tab.

Alert Central

To view system and application-defined alerts, perform the following step.

Procedure

Run RTMT to connect to the target server, then choose **Tools > Alert Central** in the **System** pane.

Figure 33: RTMT Alerts

The screenshot shows the Cisco Unified Real Time Monitoring Tool (RTMT) interface. The main window is titled "Real Time Monitoring Tool" and is currently logged into "acton-livedata2.boston.com". The "Alert Central" pane is active, displaying a table of alerts. The table has columns: Alert Name, Enabled, In Safe Range, Alert Action, Last Alert Raised, and System Cleared Time. The "Alert History" pane below shows a list of recent alerts with columns: Time Stamp, Node, Alert Name, Severity, Sent to, Description, and Group.

Alert Name	Enabled	In Safe Range	Alert Action	Last Alert Raised	System Cleared Time
IDPMetaDataLoadError	Enabled	N/A	Default	01:04:24 PM 06/30/16	N/A
IDPMetaDataUpdateError	Enabled	N/A	Default	N/A	N/A
IdSDataGridFailure	Enabled	N/A	Default	N/A	N/A
IdSInitializationFailure	Enabled	N/A	Default	N/A	N/A
IdSSecurityConfigNotPresent	Enabled	N/A	Default	N/A	N/A
IdSSecurityConfigPullFailure	Enabled	N/A	Default	N/A	N/A
IdSStateNotConfigured	Enabled	N/A	Default	01:04:24 PM 06/30/16	N/A
IdSStateOutOfService	Enabled	N/A	Default	N/A	N/A
Intelligence Center CUIC_DATABASE_UNAVA...	Enabled	Yes	Default	N/A	N/A
Intelligence Center CUIC_DB_REPLICATION...	Enabled	Yes	Default	N/A	N/A
Intelligence Center CUIC_LIVE_DATA_FEEDS...	Enabled	Yes	Default	N/A	N/A
Intelligence Center CUIC_REPORT_EXECUTI...	Enabled	Yes	Default	N/A	N/A
Intelligence Center CUIC_UNRECOVERABLE...	Enabled	Yes	Default	N/A	N/A
Intelligence Center Infrastructure_DEADLOCK...	Enabled	Yes	Default	N/A	N/A
Intelligence Center Infrastructure_LICENSE_E...	Enabled	Yes	Default	N/A	N/A
Intelligence Center Infrastructure_LICENSE_E...	Enabled	Yes	Default	N/A	N/A
Intelligence Center Infrastructure_LICENSE_...	Enabled	No	Default	02:04:24 PM 06/30/16	N/A
Intelligence Center Infrastructure_LICENSE_P...	Enabled	No	Default	02:04:24 PM 06/30/16	N/A
Intelligence Center Infrastructure_LOG_PURG...	Enabled	Yes	Default	N/A	N/A
Intelligence Center Infrastructure_PERSISTE...	Enabled	Yes	Default	N/A	N/A
Intelligence Center Infrastructure_PERSISTE...	Enabled	Yes	Default	N/A	N/A

Time Stamp	Node	Alert Name	Severity	Sent to	Description	Group
02:23:54 PM 06/30/...	acton-lived...	SyslogSeverityMatchFound	Critical	At Thu Jun 30 14:23:54 EDT 2016 on no...	System	
02:24:54 PM 06/30/...	acton-lived...	SyslogSeverityMatchFound	Critical	At Thu Jun 30 14:24:54 EDT 2016 on no...	System	
02:25:54 PM 06/30/...	acton-lived...	SyslogSeverityMatchFound	Critical	At Thu Jun 30 14:25:54 EDT 2016 on no...	System	
02:27:24 PM 06/30/...	acton-lived...	SyslogSeverityMatchFound	Critical	At Thu Jun 30 14:27:24 EDT 2016 on no...	System	
02:28:24 PM 06/30/...	acton-lived...	SyslogSeverityMatchFound	Critical	At Thu Jun 30 14:28:24 EDT 2016 on no...	System	
02:29:24 PM 06/30/...	acton-lived...	SyslogSeverityMatchFound	Critical	At Thu Jun 30 14:29:24 EDT 2016 on no...	System	
02:29:24 PM 06/30/...	acton-lived...	CriticalServiceDown	Critical	Service operational status is DOWN. C...	System	

510002

Cisco Identity Service Alerts

You can view the Cisco Identity Service alerts from the **Intelligence Center** pane.

The following table describes these alerts.

Table 73:

Alert Name	Syslog Alarm Name	Description
IdSInitializationFailure	IDS_INIT_ERROR	This alert occurs when an error is encountered during IdS initialization.
IDPMetaDataLoadError	IDP_META_DATA_LOAD_ERROR	This alert occurs when the trust could not be established between IdS and IdP during initialization.
SPMetaDataLoadError	SP_META_DATA_LOAD_ERROR	This alert occurs when SAML SP metadata Initialization fails.

IdPMetaDataUpdateError	IDP_META_DATA_UPDATE_ERROR	This alert occurs when there is an error updating IdP metadata and propagating across the cluster.
SPMetaDataUpdateError	SP_META_DATA_UPDATE_ERROR	This alert occurs when SAML SP certificate regeneration fails.
TokenMetaDataUpdateError	TOKEN_META_DATA_UPDATE_ERROR	This alert occurs when TOKEN Keystore regeneration or update fails.
IdSSecurityConfigNotPresent	IDS_SECURITY_CONFIG_NOT_PRESENT	This alert occurs when some IdS security configuration files are not present on the secondary node.
IdSSecurityConfigPullFailure	IDS_SECURITY_CONFIG_PULL_FAILURE	This alert occurs when the security config could not be pulled from the primary IdS node.
SAMLCertificateLoadFailed	SAML_CERTIFICATE_LOAD_FAILED	This alert occurs when the system is unable to read the SAML SP certificate.
IdSStateNotConfigured	STATE_NOT_CONFIGURED	This alert occurs when the trust between IdS node and IdP is yet to be established or when the IdS configuration could not be synchronized from the primary node.
IdSStateOutOfService	STATE_OUT_OF_SERVICE	This alert occurs whenever a system error results in the IdS Application failing to start.



Note To view or edit values for any alert, right-click the alert and select **Set Alert/Properties**.

Cloud Connect Syslog and Alert

Below are the set of syslog messages and alert which can be viewed from RTMT.

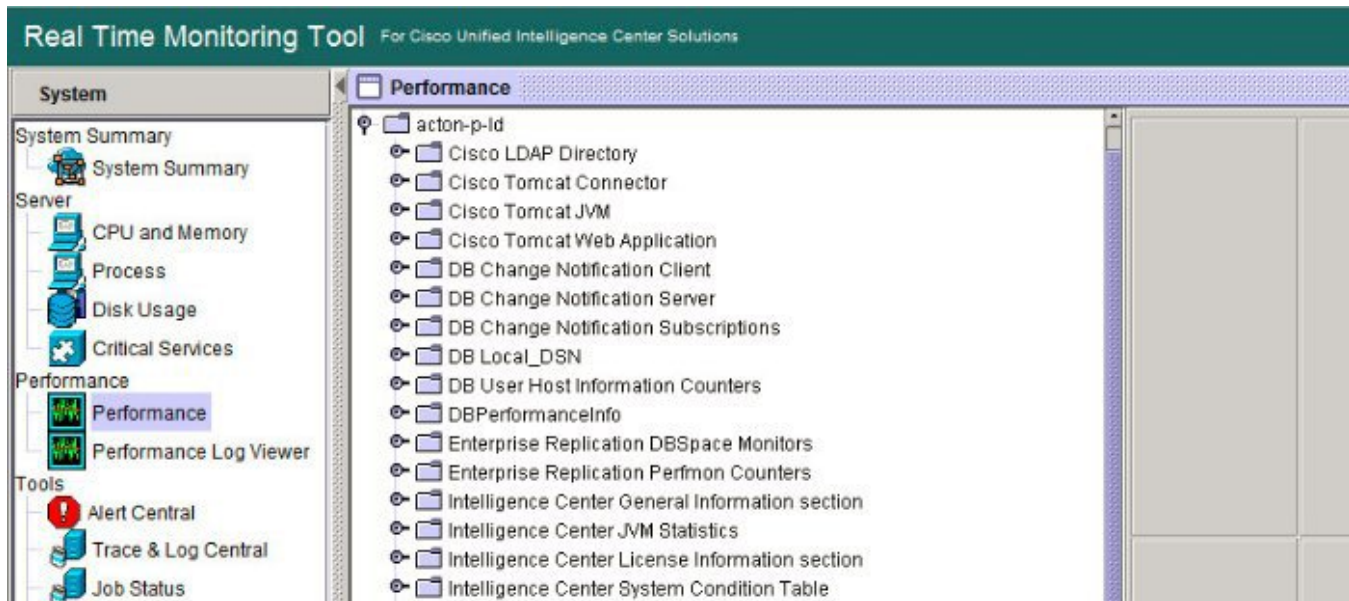
Syslog Alarm Name	Display Name in RTMT	Description
CONTM_INIT_FAILURE	ContainerManagerInitFailure	Container Manager initialisation failed
CONTM_INIT_HTTP_FAILURE	ContainerManagerInitProvisioningFailure	Container Manager HTTP Server initialisation failed
CONTM_INIT_PROVISIONING_FAILURE	ContainerManagerHTTPServerInitFailure	Container Manager fails to initialise the provisioning
SERVICE_FAILURE	CloudConnectServiceFailure	Cloud Connect Service encountered an error requiring manual intervention

View Performance Counters

Procedure

Run RTMT to connect to the target server, then choose **Performance** > **Performance** in the **System** pane.

Figure 34: RTMT Performance Interface



Disaster Recovery

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup functions.
- Scheduled backups or manual (user-invoked) backups.

To back up and restore a Unified Intelligence Center standalone or coresident (Unified Intelligence Center, Live Data, and Cisco IdS) server, see the *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/en/US/products/ps9755/prod_maintenance_guides_list.html. The procedures in the Disaster Recovery System chapter in this document also apply to the Live Data standalone, Cisco IdS standalone server and Cloud Connect.

Disaster recovery does not completely cover the Live Data application. After you complete a disaster recovery, reconfigure the Live Data application. To reconfigure Live Data, complete the tasks in the Live Data Installation procedure in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_installation_guides_list.html.



CHAPTER 11

Cloud Connect Serviceability

This section covers the serviceability information related to Cisco Web Proxy, Cloud Connect management, Digital Routing service, and DataConn service.

- [Cloud Connect Platform](#), on page 261
- [Serviceability for Web Proxy](#), on page 263
- [Serviceability for Cloud Connect Management](#), on page 264
- [Serviceability for Digital Routing](#), on page 266
- [Serviceability for DataConn](#), on page 283

Cloud Connect Platform

This chapter provides steps to collect, download and view service logs using RTMT, and purge log files using CLIs.

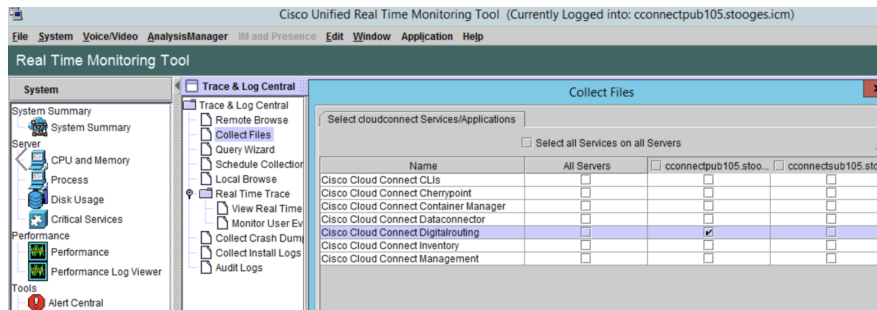
Collect service logs using RTMT

You can collect and download the service logs from the Real Time Monitoring Tool (RTMT) interface. For instructions, see the *Download Trace and Log Files* section in the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html>

Use the **Cisco Cloud Connect Digital Routing** option in the **Collect Files** page in the RTMT interface to download the Digital Routing logs.

Use the **Cisco Cloud Connect Management** option in the **Collect Files** page in the RTMT interface to download the Cloud Connect Management service logs.

Use the **Cisco Cloud Connect DataConnector** option in the **Collect Files** page in the RTMT interface to download the DataConn logs.



The service logs are downloaded to the "Downloads directory".

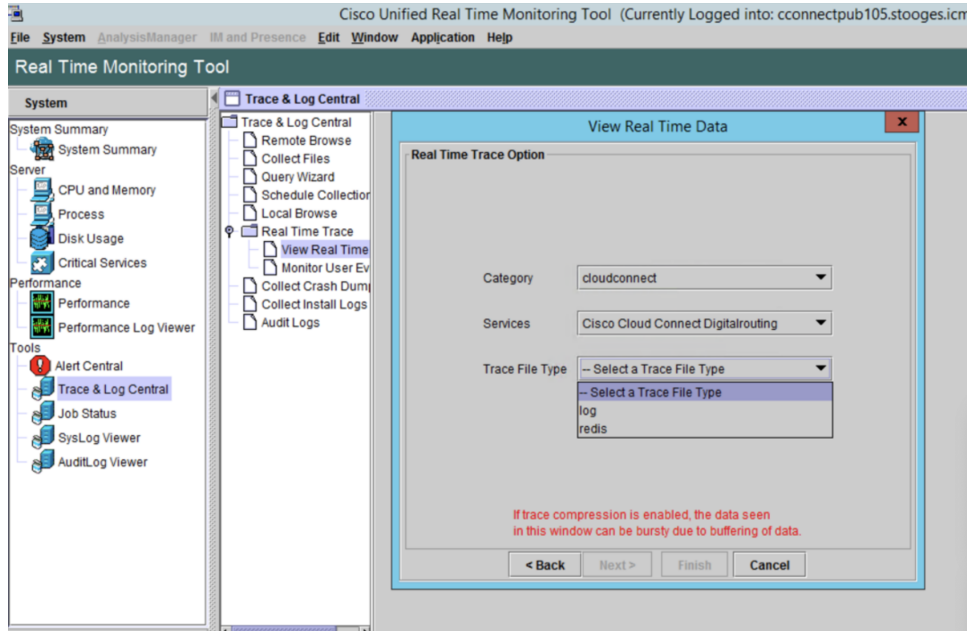
View Real-time service logs using RTMT

To view the real-time logs,

Procedure

- Step 1** Run RTMT to connect to the target server.
- Step 2** Choose **Tools > Trace & Log Central > Real Time Trace > View Real Time Data** in the **System** pane.
- Step 3** Select the **Trace File Type**. For example, select log or redis for Cloud Connect Digitalrouting.

Figure 35: Trace File Type



- Step 4** Click **Finish**.
The list of real-time log appears.

Purge log files using CLIs

You can use the CLIs to purge the hprof files created during the heap dump. Following are the CLI commands to list and delete the file:

Table 74: Purge log files using CLIs

Command	Description	Sample
file list activelog <log location that consists the files>	This lists the files in the location specified.	file list activelog hybrid\log\digitalrouting*.hprof
file delete activelog <file name >	This deletes the file in the location specified.	file delete activelog hybrid\log\digitalrouting\ <name>.hprof< td=""> </name>.hprof<>

Serviceability for Web Proxy

This section provides serviceability information for the Web Proxy service. You can set up trace levels and collect Web Proxy log information.

Set up trace levels

The admin sets the Web Proxy access-log-level.

Syntax

```
set webproxy access-log-level [option]
```

Following are the options:

- **off:** turns off the log-level access
- **info:** sets log-level access to information
- **debug:** sets log-level access to debug

Example:

```
admin:set webproxy access-log-level info
```

Output response:

```
Successfully set webproxy access log-level to info
```

Collect Web Proxy logs

You can download the logs using RTMT or file command in the admin console. You can review these logs to verify the status or any problem in the Web proxy services.

Serviceability for Cloud Connect Management

This section provides serviceability information for the Cloud Connect Management. You can configure service logging and remote syslog destinations using APIs and Command-line Interfaces (CLIs). You can view or download the log files that are stored in the Directory listing using CLI or the built-in Real Time Monitoring Tool (RTMT). You can also monitor the status of the Cloud Connect Management.

Set up trace levels

This section outlines the setting up of the trace levels for Cloud Connect Management.

To view the list of containers in the Cloud Connect, run the following command:

```
admin:utils cloudconnect list
```

To set the list of trace level for the Cloud Connect, run the following command:

```
set cloudconnect log_level [container-name] [log-level]
```

- container-name must be valid
- log-level must be a valid log level [trace|debug|info|warn|error]

For example,

```
admin:set cloudconnect log_level cloudconnectmgmt trace
```

The result for the command is as follows:

The log level will be changed to TRACE for the container cloudconnectmgmt within 30 seconds



Note The container-name and log-level must be valid. The valid log levels are [trace|debug|info|warn|error].

Download Cloud Connect Management logs

To download logs, run the following command:

```
file get activelog hybrid/log/cloudconnectmgmt/cloudconnectmgmt.log
done.
Sub-directories were not traversed.
Number of files affected: 1
Total size in Bytes: 2472833
Total size in Kbytes: 2414.876
Would you like to proceed [y/n]? y
FTP server IP: 192.168.1.105
      FTP server port [22]:
      Jser ID: root
      Password:
      *****
      Download directory:
      Transfer completed
```

View the status of Cloud Connect Management service

The status API provides the internal status of the Cloud Connect node and functional modules of the Cloud Connect Management service. The API can be used to fetch the internal state and verify status.

Cloud Connect Management services are accessed through the following status API:

- URL: <https://cloudconnectfqdn:8445/cloudconnectmgmt/status>
- Method: GET
- Content-Type: application/json
- Authentication: Basic authentication using platform credentials (username and password).

```
{
  "status": "IN_SERVICE",
  "timestamp": 1668416327203,
  "cluster": { "nodes":
    [
      {
        "address": "cconnectpub105.stooges.icm",
        "status": "MemberUp", "statusSince": 1668416327201,
        "statusUrl": "https://cloudconnectFQDN/cloudconnectmgmt/status"
      },
      {
        "address": "cconnectsub105.stooges.icm", "status": "MemberUp",
        "statusSince": 1668416327201,
        "statusUrl": "https://cloudconnectFQDN/cloudconnectmgmt/status"
      }
    ]
  },
  "isConfigWriter": true, "description": "cloudconnectmgmt Service Status Snapshot",
  "details":
  {
    "components":
    [
      {
        "name": "cloudconnectmgmt", "status": "IN_SERVICE",
        "statusSince": 1668416327202,
        "fusion": { "registration":
          {
            "status": "REGISTERED",
            "registeredSince": 1665377645055,
            "orgId": "4a2a8302-56f0-47b4-8800-45dd68104bd7",
            "clusterId": "0ddbf6d5-f949-4e2a-ab59-7dc3466ba6ea",
            "idBrokerHost": "idbrokerbts.webex.com",
            "fmsHost": "hercules-intb.ciscopark.com",
            "u2cHost": "u2c-intb.ciscopark.com"
          }
        },
        "connector":
        {
          "connectorType": "cjp_hybrid",
          "connectorVersion": "12.6.2-1.0.389",
          "status": "STARTED",
          "heartbeatFailureCount": 0,
          "lastHeartbeatTime": 1668416323571,
          "lastHeartbeatFailureTime": -1
        }
      }
    ]
  }
}
```

Serviceability for Digital Routing

This section provides serviceability information for the Digital Routing service. You can configure service logging and remote syslog destinations using APIs and Command-line Interfaces (CLIs). You can view or download the log files from the directory listing using CLI or the built-in Real Time Monitoring Tool (RTMT). You can also monitor the status of the Digital Routing service.

Additionally, you can get insights into how to access and collect the Java Management Extensions (JMX) counters using APIs or Java Monitoring and Management Console (JConsole).

Configure Service Logging

The Digital Routing service contains multiple modules. The service provides options to configure the logging levels for each of those modules independently. The default out-of-box service logging for all the modules is INFO. By default, the maximum size of each log file is 100 MB. The log files are rotated or overwritten when the accumulated file size reaches to 500 MB.

The following are the log levels for the Digital Routing service:

Log Level	Indicates
info	Informational log
debug	Debugging log
warn	Warning log
error	Error log
notice	Notification log

Configure service logging using API

You can configure the Digital Routing service log modules using API.

The following are the descriptions of the Digital Routing service log modules:

Log Module	Description
api	Logging layer for REST controller events for all the exposed APIs.
db	Logging layer for handling data sources like awdb (local database that contains configuration and real-time data) and Media Routing Domain (MRD) configuration.
security	Logging layer for handling authentication and authorization related events.
mr	Logging layer for interaction with CCE Media Routing Peripheral Gateway (MR-PG).
persistence	Logging layer for persistence to file system for configurations including replication.
logging	Logging layer for Java Management Extensions (JMX) monitoring related events.
state	Logging layer for events related to Digital Routing state machine related events.
mbeans	Logging layer for Digital Routing mbeans related traces for service counters.

servicecounter	Logging layer for Digital Routing servicecounter traces.
----------------	--

```
{
  "configuredLevel": [
    {
      "logModule": "logging",
      "logLevel": "info"
    },
    {
      "logModule": "org.springframework.security",
      "logLevel": "info"
    },
    {
      "logModule": "org.springframework",
      "logLevel": "info"
    },
    {
      "logModule": "api",
      "logLevel": "info"
    },
    {
      "logModule": "db",
      "logLevel": "info"
    },
    {
      "logModule": "mr",
      "logLevel": "info"
    },
    {
      "logModule": "security",
      "logLevel": "info"
    },
    {
      "logModule": "state",
      "logLevel": "info"
    },
    {
      "logModule": "persistence",
      "logLevel": "info"
    },
    {
      "logModule": "jmx",
      "logLevel": "info"
    },
    {
      "logModule": "redisclient",
      "logLevel": "info"
    },
    {
      "logModule": "mbeans",
      "logLevel": "info"
    },
    {
      "logModule": "servicecounter",
      "logLevel": "info"
    }
  ]
}
```

Digital Routing trace

The following are the API details to view the Digital Routing service trace:

- URL: <https://hostname/draapi/v1/config/trace/dr>

- Method: GET, PUT
- Content-Type: application/json
- Authentication: Basic authentication using platform credentials (username and password).

GET Response:

```
{
  "syslogConfig": {
    "primary-host": "",
    "secondary-host": "",
    "logLevel": "info"
  }
}
```

PUT Payload

```
{
  "syslogConfig": {
    "primary-host": "<Primary SyslogIP>"
    "secondary-host": "<<Secondary SyslogIP>"",
    "logLevel": "debug"
  }
}
```

Redis service trace

The following are the API details to view the Redis service trace:

- URL: https://host_fqdn:8445/drapiv1/config/trace/redis
- Method: GET,PUT
- Content-Type: application/json
- Authentication: Basic authentication using platform credentials (username and password).

GET Response:

```
[
  "loglevel",
  "notice"
]
```

PUT Payload:

```
{
  "redisConfiguredLevel": "<notice|debug|verbose|warning>"
}
```

Configure service logging using CLI

To configure the service logging for the Digital Routing service and the Redis service traces using CLI:

Digital Routing service trace

To configure the Digital Routing service trace, run the following command:

```
utils cloudconnect digitalrouting logging trace set drapi <info|debug|warn|error>
```

To view the Digital Routing service trace list, run the following command:

```
utils cloudconnect digitalrouting logging trace list drapi
```

The list of Digital Routing service trace appears.

Redis service trace

To configure the Redis service trace, run the following command:

```
utils cloudconnect digitalrouting logging trace set redis <notice|warning|verbose|debug>
```

To view the Redis service trace, run the following command:

```
utils cloudconnect digitalrouting logging trace list redis
```

The list of Digital Routing service trace appears.

Configure syslog

Digital Routing service provides the option to configure remote syslog destinations. It allows configuration for up to two remote destinations. The default out-of-box syslog remote destinations are empty and on deployment, it requires accurate configuration.

Configure syslog using API

The following are the API details to configure the destination where the syslogs are stored:

- URL: https://host_fqdn:8445/drapi/v1/config/trace/syslog
- Method: GET, PUT
- Content-Type: application/json
- Authentication: Basic authentication using platform credentials (username and password).

GET Response

```
{
  "syslogConfig": {
    "primary-host": "",
    "secondary-host": "",
    "logLevel": "info"
  }
}
```

PUT Payload

```
{
  "syslogConfig": {
    "primary-host": "<Primary SyslogIP>"
    "secondary-host": "<<Secondary SyslogIP>"",
    "logLevel": "debug"
  }
}
```

Configure syslog using CLI

Digitalrouting provides the ability to configure remote syslog servers through which specified system logs are generated. You can access the syslog from the syslog server.

To configure syslogs, run the following command:

```
utils cloudconnect digitalrouting logging syslog set <primary-host|secondary-host> %host address%
```

- primary-host: Use this keyword when you are setting the primary syslog server hostname.
- secondary-host: Use this keyword when you are setting the secondary syslog server hostname.
- host address: Refers to the remote syslog server IP address or hostname or fqdn.

Once you run the command to configure syslogs, you will get the message in your command prompt as below:

The syslog configurations are successfully updated.

To view the syslog list, run the following command:

```
utils cloudconnect digitalrouting logging syslog list
```

The list of syslogs that are logged for the Digital Routing service appears.

To view the trace list syslog, run the following command:

```
utils cloudconnect digitalrouting logging trace list syslog
```

The trace list syslogs that are logged for the Digital Routing service appears.

To update log trace set, run the following command:

```
utils cloudconnect digitalrouting logging trace set syslog %loglevel%
```

The Cloud Connect Digital Routing logging trace set syslog debug successfully updated.



Note Log level options are error, warn, info, and debug.

Monitor the status of the Digital Routing service

Digital Routing services are monitored through the log collection and Java Management Extensions (JMX) counters.

The following are the API details to monitor the service status:

- URL: https://host_fqdn:8445/drap/v1/status
- Method: GET
- Content-Type: application/json
- Authentication: Basic authentication using platform credentials (username and password).

The status is INACTIVE when the connector is started, and all services are initializing and making connections. The status is ACTIVE when the connector is started and connected with all the components.


```

{
  "status": "ACTIVE",
  "cluster": {
    "nodes": [
      {
        "address": "CloudConnect local FQDN or IP",
        "status": "MemberReachable",
        "statusSince": 1664305403815,
        "statusURL": "https://<CloudConnect local FQDN or IP>:8445/drapiv1/status"
      },
      {
        "address": "CloudConnect remote FQDN or IP",
        "status": "MemberReachable",
        "statusSince": 1662189184290,
        "statusURL": "https://<CloudConnect remote FQDN or IP>:8445/drapiv1/status"
      }
    ]
  },
  "description": "digitalrouting Service Status Snapshot",
  "details": {
    "components": [
      {
        "name": "digitalrouting",
        "status": "ACTIVE",
        "statusSince": 1664305429343
      },
      {
        "name": "redis",
        "status": "MASTER",
        "statusSince": 1664305423670
      }
    ]
  },
  "apiLatencyResponseinMs": {
    "avgCurrentResponse": 0,
    "avgPreviousResponse": 0,
    "avgTodayResponse": 0,
    "avgServiceUpResponse": 0
  }
}

```

Download logs using CLI

To download logs, run the following command:

```

admin: file get acti
admin: file get activelog hybrid/log/digitalrouting/dr-app-*.log
lease wait while the system is gathering files info
Get file: active/hybrid/log/digitalrouting/dr-app-2022-08-04-051932.log
Get file: active/hybrid/log/digitalrouting/dr-app-2022-08-04-051934.log
Get file: active/hybrid/log/digitalrouting/dr-app-2022-08-04-092115.log
Get file: active/hybrid/log/digitalrouting/dr-app-2022-08-04-092116.log
done.
subdirectories were not traversed.
Number of files affected: 12

```

```

Total size in Bytes: 2434450
Total size in Kbytes: 2377.3926
Would you like to proceed [y/n]?
Y
FTP server IP: 192.168.1.105
FTP server port [22]:
Juser ID: root
Password:
*****
Download directory:
Transfer completed
admin•

```

Directory listing

The directory listing page provides the path to the log files with the file name, file size, and last modified details. You can click on a file name to access the log file.

The path to access the log directory for Digital Routing service is as follows:

https://host_fqdn:8445/drapl/log/digitalrouting

The path to access the log directory for Platform files is as follows:

https://host_fqdn:8445/drapl/common/log

Access JMX counters

You can access the Java Virtual Machine (JVM) counters, Service counters, and Redis counters using either APIs or JConsole.

Access JMX Counters using API

To access the JMX counters using API:

JVM counters

The following are the API details to access the JVM counters:

- URL: https://host_fqdn:8445/drapl/v1/metrics/jvmcounters
- Method: GET
- Content-Type: application/json
- Authentication: Basic authentication using platform credentials (username and password).

```

{
  "java.lang:type=Memory": {
    "name": "java.lang:type=Memory",

```

```

    "attribute": {
      "HeapMemoryUsage": "{committed=1073741824, init=1073741824, max=1719664640,
used=365429248}",
      "NonHeapMemoryUsage": "{committed=141688832, init=2555904, max=1056964608,
used=134275968}"
    }
  },
  "java.lang:type=OperatingSystem": {
    "name": "java.lang:type=OperatingSystem",
    "attribute": {
      "ProcessCpuTime": "6314000000",
      "SystemCpuLoad": "0.1756357022315391",
      "CommittedVirtualMemorySize": "2839908352",
      "AvailableProcessors": "2",
      "FreePhysicalMemorySize": "1289973760",
      "ProcessCpuLoad": "0.0",
      "TotalPhysicalMemorySize": "2147483648"
    }
  },
  "java.lang:type=Threading": {
    "name": "java.lang:type=Threading",
    "attribute": {
      "ThreadCount": "210",
      "PeakThreadCount": "210",
      "CurrentThreadCpuTime": "221284760"
    }
  }
}

```

Service counters

The following are the API details to access the JMX Service counters:

- URL: https://host_fqdn:8445/draapi/v1/metrics/servicecounters
- Method: GET
- Content-Type: application/json
- Authentication: Basic authentication using platform credentials (username and password).

```

{
  "DraapiServiceCountersPreviousInterval30Minutes": {
    "name": "DraapiServiceCountersPreviousInterval30Minutes",
    "attribute": {
      "TasksAbandonedAgent": "0",
      "TasksAbandonedCustomer": "0",
      "TasksAccepted": "0",
      "TasksCompleted": "0",
      "TasksReceived": "0",
      "TasksRejected": "0",
      "TasksRejectedCCERouter": "0",
      "TasksRouted": "0",
      "TasksTransferred": "0",
      "WebhookNotify": "0",
      "WebhookNotifyFailed": "0"
    }
  },
  "DraapiServiceCountersToday": {
    "name": "DraapiServiceCountersToday",
    "attribute": {
      "TasksAbandonedAgent": "0",
      "TasksAbandonedCustomer": "0",
      "TasksAccepted": "0",

```

```

    "TasksCompleted": "0",
    "TasksReceived": "0",
    "TasksRejected": "0",
    "TasksRejectedCCERouter": "0",
    "TasksRouted": "0",
    "TasksTransferred": "0",
    "WebhookNotify": "0",
    "WebhookNotifyFailed": "0"
  }
},
"Time": {
  "requestReceivedTime": "22 Nov 2022 03:11:03.574 UTC"
},
"DrapiServiceCountersSinceServiceUp": {
  "name": "DrapiServiceCountersSinceServiceUp",
  "attribute": {
    "TasksAbandonedAgent": "0",
    "TasksAbandonedCustomer": "0",
    "TasksAccepted": "0",
    "TasksCompleted": "0",
    "TasksReceived": "3",
    "TasksRejected": "3",
    "TasksRejectedCCERouter": "0",
    "TasksRouted": "0",
    "TasksTransferred": "0",
    "WebhookNotify": "0",
    "WebhookNotifyFailed": "0"
  }
},
"DrapiServiceCountersCurrentInterval30Minutes": {
  "name": "DrapiServiceCountersCurrentInterval30Minutes",
  "attribute": {
    "TasksAbandonedAgent": "0",
    "TasksAbandonedCustomer": "0",
    "TasksAccepted": "0",
    "TasksCompleted": "0",
    "TasksReceived": "0",
    "TasksRejected": "0",
    "TasksRejectedCCERouter": "0",
    "TasksRouted": "0",
    "TasksTransferred": "0",
    "WebhookNotify": "0",
    "WebhookNotifyFailed": "0"
  }
},
"DrapiServiceCountersRealTime": {
  "name": "DrapiServiceCountersRealTime",
  "attribute": {
    "ChatTasksInDrapiQueue": "0",
    "EmailTasksInDrapiQueue": "0",
    "RunApplicationScriptThrottleCount": "0",
    "SocialTasksInDrapiQueue": "0",
    "TasksInCCEQueue": "0",
    "TasksInDrApiQueue": "0",
    "TasksInWebhookNotificationQueue": "0",
    "TelephonyTasksInDrapiQueue": "0"
  }
}
}

```

Redis counters

The following are the API details to access the Redis counters:

- URL: https://host_fqdn:8445/drap/v1/metrics/rediscounters

- Method: GET
- Content-Type: application/json
- Authentication: Basic authentication using platform credentials (username and password).

```
{
  "redis_version": "6.2.7",
  "redis_mode": "standalone",
  "os": "Linux 3.10.0-1160.53.1.el7.x86_64 x86_64",
  "arch_bits": "64",
  "gcc_version": "10.3.1",
  "server_time_usec": "1664456513263005",
  "uptime_in_seconds": "94",
  "uptime_in_days": "0",
  "connected_clients": "9",
  "maxclients": "10000",
  "blocked_clients": "1",
  "used_memory_human": "1.26M",
  "used_memory_rss_human": "4.54M",
  "used_memory_peak_human": "1.28M",
  "used_memory_peak_perc": "98.98%",
  "used_memory_overhead": "992439",
  "used_memory_startup": "846815",
  "used_memory_dataset": "333195",
  "used_memory_dataset_perc": "69.59%",
  "total_system_memory_human": "9.61G",
  "used_memory_lua_human": "77.00K",
  "used_memory_scripts_human": "9.01K",
  "maxmemory_human": "0B",
  "maxmemory_policy": "noeviction",
  "mem_fragmentation_ratio": "4.28",
  "mem_fragmentation_bytes": "3645653",
  "mem_replication_backlog": "0",
  "mem_clients_slaves": "0",
  "mem_clients_normal": "136138",
  "total_connections_received": "89",
  "total_commands_processed": "942",
  "instantaneous_ops_per_sec": "9",
  "total_net_input_bytes": "145705",
  "total_net_output_bytes": "48704",
  "instantaneous_input_kbps": "0.24",
  "instantaneous_output_kbps": "0.07",
  "rejected_connections": "0",
  "evicted_keys": "0",
  "role": "master",
  "connected_slaves": "0",
  "master_failover_state": "no-failover",
  "master_replid": "400fbf197d0ac2375ee9eafddc4fcf539fa8e7e0",
  "master_replid2": "feb0f97258906cad43eba1657bdf28419d1348af",
  "master_repl_offset": "0",
  "second_repl_offset": "1",
  "repl_backlog_active": "0",
  "repl_backlog_size": "1048576",
  "repl_backlog_first_byte_offset": "0",
  "repl_backlog_histlen": "0",
  "used_cpu_sys": "0.117309",
  "used_cpu_user": "0.077111",
  "errorstat_ERR": "count=52"
}
```

Access Counters using JConsole

Following are the JMX counters you can access using the JConsole:

- JVM counters
- Service counters
- Redis counters

For instruction about how to access JConsole, see the *Using JConsole* section available at <https://openjdk.org/tools/svc/jconsole/>

JVM counters

You can access JVM counters of the following mbeans type: Memory, Operating System, and Threading.

To access the JVM **Memory** counter attributes:

1. Navigate to **java.lang > java.lang > Memory > Attributes**. Jconsole opens to provide the IP address of cloud-connect box and port 10006.
2. Navigate to the **MBeans** tab > **java.lang > Memory > Attributes** to view the list of attributes.

To access the JVM **Operating System** counter attributes:

1. Navigate to **java.lang > java.lang > Operating System > Attributes**. Jconsole opens to provide the IP address of cloud-connect box and port 10006.
2. Navigate to the **MBeans** tab > **java.lang > Operating System > Attributes** to view the list of attributes.

To access the JVM **Threading** counter attributes:

1. Navigate to **java.lang > java.lang > Threading > Attributes**. Jconsole opens to provide the IP address of cloud-connect box and port 10006.
2. Navigate to the **MBeans** tab > **java.lang > Threading > Attributes** to view the list of attributes.

Service counters

To access the Digital Routing Service counters:

1. Navigate to **com.cisco.ccbu.dr.mbeans > Drapi Mxbean Counter**.

Following are the **MxBean** counters available:

- a. drapicountersCurrentIntervalMXBean
- b. drapicountersPreviousIntervalMxBean
- c. drapicountersRealTimeMXBean
- d. drapicountersServiceUpMXBean
- e. drapicountersTodayMXBean

2. Click **Attributes** to view the Service counter attributes.

3. Click on an *Attribute* to view the attribute value.

Redis counters

To access the Digital Routing specific Redis counters:

1. Navigate to **com.cisco.ccbu.dr.mbeans** > **RedisMXBean** > **Attributes**.
2. Click on an *Attribute* to view the attribute value.

Access Digital Channel Statistics in CCE Administration Portal

To access the statistics for Digital Channel and Redis service running on the Cloud Connect:

Procedure

In **Unified Contact Center Enterprise Management**, navigate to **Overview** > **Digital Channels** > **Digital Channel Statistics**.

The Digital Channel Statistics page displays the Digital Routing and Redis service Host, Status, Role, and Up Since.

The Task Information section displays the Realtime tasks, Historical tasks with duration of each task.

The Realtime Tasks displays the Tasks in Digital Routing Queue and the Tasks in CCE Routing Queue.

The Historical Tasks section displays the duration of the current and previous task.

The historical task statuses are *Received*, *Rejected*, *Rejected by CCE*, *Queued*, *Route requests*, *Close requests*, *Transfer requests*, *Abandoned by customer*, and *Failed webhook requests*.

For more information, refer to the descriptions for [JMX Service counter definitions](#), on page 277 in the *Cloud Connect Serviceability* section of the [Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise](#).

JMX Service counter definitions

The following table provides the Java Management Extensions (JMX) Service counter definitions:

Table 75: JMX Service counter definitions

JMX Counters	Label in CCE Administration Portal	Current Interval (default 30 minutes interval)	Previous Interval	Today (24 hours)	Since Service Up	Real-time
TasksReceived	Received	The counter increments for every incoming task. The counter resets after every interval.	The number of incoming tasks in the current interval is updated to the previous interval at the interval cutover.	The total number of tasks of all the previous interval for the day + the number of injected tasks in the current interval.	The total number of all the previous interval incoming tasks of the day + the number of task received in the current interval.	TasksReceived CallsQueued The counter increments when a new task changes from CREATED to QUEUED state. The counter decrements when the task changes from QUEUED to ROUTED or CLOSED.
TasksAccepted	Queued	The counter increments for the tasks in the CREATED state and continues to increment for every incoming task updated to CREATED state. The counter resets after every interval.	The number of current interval task in the CREATED state updated to task accepted in the previous interval at the interval cutover.	The total number of tasks of all previous interval in the CREATED state for the day + the number of task accepted in the current interval.	The total number of all previous interval incoming task in the CREATED state + the number of tasks accepted in the current interval.	TasksAccepted ClientRequestQueue The <i>ClientRequestQueue</i> size provides the real-time counter value of incoming task accepted.

JMX Counters	Label in CCE Administration Portal	Current Interval (default 30 minutes interval)	Previous Interval	Today (24 hours)	Since Service Up	Real-time
TasksCompleted	Close requests	The counter increments the number of normally closed tasks and continues to increment for every closed task. The counter resets after every interval.	The number of current interval tasks in the CLOSED state with normal disposition updated to TaskCompleted in the previous interval at the interval cutover.	The total number of tasks in CLOSED state with normal disposition for the day + the TasksCompleted in the current interval.	The total number of all previous interval incoming task in the CLOSED state with normal disposition + the number of tasks completed in the current interval.	TasksInWebhookNotificationQueue The <i>RedissonQueues</i> size provides the real-time counter value of the task in <i>WebhookNotificationQueue</i>
TasksRouted	Route requests	The counter increments the number of tasks in the ROUTED state and continues to increment the counter for every task updated to ROUTED state. The counter resets after every interval.	The number of tasks in the ROUTED state in the current interval is updated to TasksRouted in the previous interval at the interval cutover.	The total number of all previous interval tasks which are updated to ROUTED for the day+ the number of TasksRouted in the current interval.	The total number of all previous interval incoming task in the ROUTED state + the number of tasks routed in the current interval.	ClientRequestQueue The <i>ClientRequestQueue</i> size provides the real-time counter value of incoming accepted task for media type chat.

JMX Counters	Label in CCE Administration Portal	Current Interval (default 30 minutes interval)	Previous Interval	Today (24 hours)	Since Service Up	Real-time
TasksTransferred	Transfer requests	The counter increments incoming tasks in the TRANSFERRED state and continues to increment for every incoming transferred task. The counter resets after every interval.	The number of incoming Tasks in TRANSFERRED state in the current interval is updated to TasksTransferred in the previous interval at the interval cutover.	The total number of all previous interval incoming task in the TRANSFERRED state for the day + the number of task transferred in the current interval.	The total number of all previous interval incoming task in the TRANSFERRED state + the number of tasks transferred in the current interval.	FinalDisqQue The <i>ClientRequestQueue</i> size provides the realtime counter value of incoming accepted task for media type email.
TasksAbndnAgnt	NA	The counter increments closed task with disposition 37 and continues to increment for every closed task with the disposition 37. The counter resets after every interval.	The number of closed tasks with disposition 37 in the current interval is updated to TasksAbndnAgnt in the previous interval at the interval cutover.	The total number of closed task of all previous interval with disposition 37 for the day + the number of TasksAbndnAgnt in the current interval.	The total number of all previous interval closed tasks with disposition 37 + the number of TasksAbndnAgnt in the current interval.	FinalDisqQue The <i>ClientRequestQueue</i> size provides the real-time counter value of incoming accepted task for media type social.

JMX Counters	Label in CCE Administration Portal	Current Interval (default 30 minutes interval)	Previous Interval	Today (24 hours)	Since Service Up	Real-time
TasksAbandoned	Abandoned by customer	The counter increments the number of closed tasks with disposition 29 and continues to increment the counter for every closed task with disposition 29. The counter resets after every interval.	The number of closed Tasks with disposition 29 in the current interval is updated to TasksAbandoned in the previous interval at the interval cutover.	The total number of closed tasks all the previous interval with disposition 29 for the day + the number of TasksAbandoned in the current interval.	The total number of all previous interval closed tasks with disposition 29 + the number of TasksAbandoned in the current interval.	TasksAbandoned The ClientRequestQueue size provides the real-time counter value of incoming accepted task for media type telephony.
TasksRejected	Rejected	The counter increments the number of incoming tasks rejected due to the maximum limit of ClientRequestQueue size and failure of authentication. The counter resets after every interval.	The number incoming Tasks rejected due to maximum limit of ClientRequestQueue size and failure of authentication. The number of tasks in the current interval is updated to TasksRejected in the previous interval at the interval cutover.	The total number of all the previous interval incoming tasks rejected for the day due to maximum limit of ClientRequestQueue size and failure of authentication + the number of rejected task in the current interval.	The total number of all previous interval tasks dropped due to max limit of ClientRequestQueue size and Authentication failure + the number of TasksRejected in the current interval.	TasksRejected The DRAPI service can receive RNVAADNSRHC message from Media Routing (MR) Protocol Independent Multicast (PIM) and this counter increments whenever service receives more than six RNVAADNSRHC

JMX Counters	Label in CCE Administration Portal	Current Interval (default 30 minutes interval)	Previous Interval	Today (24 hours)	Since Service Up	Real-time
RejectedCCERouter	Rejected by CCE	The counter increments the number of incoming tasks rejected at the CCE router. The counter resets after every interval.	The number of incoming tasks rejected at the CCE router. The counter resets after every interval.	The number of incoming tasks rejected at the CCE router. The counter resets after every interval.	The total number of all previous interval incoming tasks rejected in CCE due to new task failure + the number of RejectedCCERouter in the current interval.	
WebhookNotify	NA	The counter increments the number of Webhook notifications sent successfully to the Webex Connect. The counter resets after every interval.	The number of Webhook notifications sent successfully to the Webex Connect is updated to WebhookNotify in the previous interval at the interval cutover.	The total number of all the previous interval Webhook notifications sent successfully to the Webex Connect for the day + the number of WebhookNotify in the current interval.	The total number of all previous interval Webhook notifications sent successfully to WebexConnect + the number of WebhookNotify in the current interval.	
WebhookNotifyFail	Failed Webhook requests	The number of Webhook notifications failed to send successfully to WebexConnect. The counter resets after every interval.	The number of Webhook notifications failed to send successfully to WebexConnect is updated to WebhookNotifyFail in the previous interval at the interval cutover.	The number of all previous interval Webhook notifications failed to send successfully to WebexConnect for the day + number of WebhookNotifyFail in the current interval.	The number of all previous interval Webhook notifications failed to send successfully to WebexConnect + the number of WebhookNotifyFail in the current interval.	

Serviceability for DataConn

This section provides serviceability information for the Cloud Connect DataConn. You can view or download the log files that are stored in the directory listing using the Real Time Monitoring Tool (RTMT). You can also monitor the status of the cloud connect DataConn.

Download DataConn logs

To download logs, run the following command:

```
file get activelog hybrid/log/cloudconnectmgmt/dataconn.log
```

The downloaded log details are displayed.

```
done.
Sub-directories were not traversed.
Number of files affected: 1
Total size in Bytes: 2472833
Total size in Kbytes: 2414.876
Would you like to proceed [y/n]? y
FTP server IP: 192.168.1.105
      FTP server port [22]:
      Jser ID: root
      Password:
      *****
      Download directory:
      Transfer completed
```

Monitor the status of DataConn service

DataConn services are monitored through status API.

The following are the API details to monitor the service status:

- URL: <https://cloudconnectfqdn:8445/dataconn/status>
- Method: GET
- Content-Type: application/json
- Authentication: Basic authentication using platform credentials (username and password).

The following is the output of status API:

```
{
  "status": "IN_SERVICE",
  "timestamp": 1681814206313,
  "cluster": {
    "nodes": [
      {
        "address": "cconnectpub105.stooges.icm",
        "status": "MemberUp",
        "statusSince": 1681814206299,
        "statusUrl": "https://cconnectpub105.stooges.icm:8445/dataconn/status"
      },
      {
        "address": "cconnectsub105.stooges.icm",
        "status": "MemberUp",
```

```
        "statusSince": 1681814206299,  
        "statusUrl": https://cconnectsub105.stooges.icm:8445/dataconn/status  
    }  
  ]  
},  
"isConfigWriter": true,  
"description": "Service Status Snapshot",  
"details": {  
  "components": [  
    {  
      "name": "UserSync",  
      "status": "IN_SERVICE",  
      "statusSince": 1681784668359,  
      "userSync": "STARTED",  
      "syncEnabled": true  
    }  
  ]  
}  
}
```



CHAPTER 12

Live Data Serviceability

- [Live Data Reporting System, on page 285](#)
- [Live Data Collecting Logs, on page 285](#)
- [Live Data Failover Configuration, on page 291](#)
- [Live Data Syslog, on page 293](#)
- [Monitor and Analyze System Performance Using Nmon, on page 294](#)
- [Live Data Socket.IO, on page 295](#)
- [Live Data SNMP, on page 296](#)

Live Data Reporting System

In Real Time data collection, reporting data writes to the Unified CCE Data Server and Unified Intelligence Center queries the data periodically. In contrast, Live Data continuously processes agent and call events from the peripheral gateway and the router, and publishes data directly to Unified Intelligence Center. Live Data continuously pushes only changed data to the reporting clients without the delay of writing to, and reading from the database. Individual state values, such as agent states, refresh as they happen, while other values, such as calls in queue, refresh approximately every 3 seconds.

The Live Data report templates take advantage of the Live Data service.

The Real Time data flow is still used to support other stock and custom reports.

Live Data is a stream processing system which aggregates and processes the events in-stream and publishes the information. Unified Intelligence Center subscribes to the message stream to receive the events in real-time and continuously update the Live Data report.

Live Data Collecting Logs

The logs that the Live Data services generate are available through the same tools as the Unified Intelligence Center logs.

For example, you can use the **file get** CLI command to collect all the Live Data logs:

```
file get activelog livedata/logs/**
```

You can also use the Real Time Monitoring Tool (RTMT) to collect and view logs and traces of the Live Data services.

Live Data Log Levels

Use the command-line interface to set trace level settings for Live Data services. There is no method in OAMP to set the log levels for the Live Data components.

You can use the **set live-data trace** command to set the log level or apply a tracemask to the following subsystems:

- Communications - logs messages related to connections
- DataProcessing - logs messages related to the processing of messages
- Database - logs messages specific to the database
- Event-store - logs messages specific to the storage of agent call-log and state-log events



Note You cannot apply a tracemask to the event-store subsystem.

Setting the loglevel

Required Minimum Privilege Level: Advanced

Command Syntax

```
set live-data trace subsystem loglevel value  
subsystem
```

communications, dataprocessing, event-store or database

value

The loglevel for the specified subsystem:

- DEBUG
- INFO
- NOTICE
- WARN
- ERROR
- CRITICAL
- ALERT
- EMERGENCY



Note Only the following log levels are applicable to the event-store subsystem: DEBUG, INFO, WARN, and ERROR.

Example: `admin:set live-data trace dataprocessing loglevel DEBUG`

Setting the tracemask

Required Minimum Privilege Level: Advanced

You can set detailed log levels by enabling trace flags, which allows debug statements to appear in the logs. You can control debug tracing for specific functionalities by specifying a TRACE flag name within specific subsystem components. See Infrastructure Trace Definitions in the *Administration Console User Guide for Cisco Unified Intelligence Center* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html>.

Command Syntax

```
set live-data trace subsystem tracemask value
subsystem
```

communications, dataprocessing, or database

value

For each of the three subsystems specify one of several tracemasks:

dataprocessing

- TIP_APPL_MESSAGE_TRACEMASK
- CAMEL_JMS_TRACEMASK
- STORM_SPOUT_TRACEMASK
- TIP_PROTOCOL_TRACEMASK
- FAILOVER_HB_TRACEMASK

database

- DB_UCCE_AW_TRACEMASK

communications

- JMS_COMMUNICATION_TRACEMASK
- FAILOVER_TOS_TRACEMASK

To set multiple tracemasks, separate them with a space.

Example: admin: set live-data trace dataprocessing tracemask TIP_APPL_MESSAGE_TRACEMASK CAMEL_JMS_TRACEMASK

To clear all tracemasks, use the tracemask command without parameters, for example:

```
set live-data trace dataprocessing tracemask
```

You can list the trace masks available for each subsystem using the command help option, for example:

```
set live-data trace dataprocessing tracemask ?
```

Show the loglevel

Required Minimum Privilege Level: Ordinary

To display the current loglevel or tracemask, use the `show live-data trace` command, for example:

```
admin:show live-data trace dataprocessing loglevel
```

```
admin:show live-data trace dataprocessing tracemask
```

Set Live-Data Trace Agent

Required Minimum Privilege Level: Advanced

Use this command to enable detailed tracing for specific agents.



Note This command requires in-depth system knowledge. Use detailed tracing only for advanced troubleshooting. Enabling detailed tracing adds many messages to the log files. The system may quickly exceed limits on the size and number of log files, causing the oldest log files to be overwritten. As a result, running detailed tracing shortens the history covered by the log files.

Command Syntax

set live-data trace agent *AgentSkillTargetIDs*
AgentSkillTargetIDs

The AgentSkillTargetIDs of the agents you want to trace. Separate IDs with a space. You can only have detailed tracing enabled for three agents simultaneously.



Note Running this command overwrites any previous setting.

Example: admin:set live-data trace agent 5037 6000

Output: Enable detailed traces for agent(s) with the following id(s): 5037 6000

Show Agents Currently Set

Required Minimum Privilege Level: Ordinary

This command shows the IDs of the agents that have detailed trace turned on.

show live-data trace agent

No parameters are required.

Example: admin:show live-data trace agent

Output: Detailed traces are turned on for the agent(s) with the following id(s): 5037

Unset Trace

Required Minimum Privilege Level: Advanced

This command turns off detailed traces for all agents.

unset live-data trace agent

No parameters are required.

Example: admin:unset live-data trace agent

Output: Disable detailed traces for all agent(s)

Help Command

unset live-data trace agent ?

Example: admin:set live-data trace agent ?

Output: This command is used to set the trace level for Agents.

Set Live-Data Trace Skill-Group

Required Minimum Privilege Level: Advanced

Use this command to enable detailed tracing for specific skill-groups.



Note This command requires in-depth system knowledge. Use detailed tracing only for advanced troubleshooting. Enabling detailed tracing for a skill-group with many agents, for example, more than one hundred, adds a large number of messages to the log files. The system may quickly exceed limits on the size and number of log files, causing the oldest log files to be overwritten. As a result, running detailed tracing shortens the history covered by the log files.

Command Syntax

set live-data trace skill-group *Skill-GroupSkillTargetIDs*
Skill-GroupSkillTargetIDs

The Skill-GroupSkillTargetIDs of the skill-groups you want to trace. Separate IDs with a space. You can only have detailed tracing enabled for 3 skill-groups simultaneously.



Note Running this command overwrites any previous setting.

Example: `set live-data trace skill-group 5037 6000`

Output: `Enable detailed traces for skill-group(s) with the following id(s): 5037 6000`

Show Skill-Groups Currently Set

Required Minimum Privilege Level: Ordinary

show live-data trace skill-group

No parameters are required.

Example: `admin:show live-data trace skill-group`

Output: `Detailed traces are turned on for the skill-group(s) with the following id(s): 11962`

Unset Trace

Required Minimum Privilege Level: Advanced

This command turns off detailed tracing for all skill-groups.

unset live-data trace skill-group

No parameters are required.

Example: `admin:unset live-data trace skill-group`

Output: `Disable detailed traces for all skill-group(s)`

Help Command

unset live-data trace skill-group ?

Example: admin:set live-data trace skill-group ?

Output: This command is used to set the trace level for skill-groups.

Set Live-Data Trace Precision-Queue

Required Minimum Privilege Level: Advanced

Use this command to enable tracing for specific precision-queues.



Note This command requires in-depth system knowledge. Use detailed tracing only for advanced troubleshooting. Enabling detailed tracing for a precision-queue adds many messages to the log files. The system may quickly exceed limits on the size and number of log files, causing the oldest log files to be overwritten. As a result, running detailed tracing shortens the history covered by the log files.

Command Syntax

set live-data trace precision-queue *Precision-QueueIDs*
Precision-QueueIDs

The Precision-QueueIDs of the precision-queues you want to trace. Separate IDs with a space. You can only have detailed tracing enabled for 3 precision-queues simultaneously.



Note Running this command overwrites any previous setting.

Example: admin:set live-data trace precision-queue 5037 6000

Output: Enable detailed traces for precision-queue(s) with the following id(s): 5037 6000

Show Precision-Queues Currently Set

Required Minimum Privilege Level: Ordinary

Show the IDs of the precision-queues that have detailed trace turned on.

show live-data trace precision-queue

No parameters are required.

Example: admin:show live-data trace precision-queue

Output: Detailed traces are turned on for the precision-queue(s) with the following id(s):
 5000

Unset Trace

Required Minimum Privilege Level: Advanced

This command turns off detailed traces for all precision-queues.

unset live-data trace precision-queue

No parameters are required.

Example: admin:unset live-data trace precision-queue

Output: Disable detailed traces for all precision-queue(s)

Help Command

unset live-data trace precision-queue ?

Example: admin:set live-data trace precision-queue ?

Output: This command is used to set the trace level for precision-queues.

Live Data Failover Configuration

The following Live Data failover commands are provided to allow you to monitor the Live Data failover mechanism during troubleshooting.

By default, Live Data failover is automatically configured during installation or upgrade. Under general operations you do not need to use these commands. Use **show live-data failover** to display information on the current configuration and state of Live Data reporting system cluster. Use **set live-data failover** to enable Live Data failover, and **unset live-data failover** to unset Live Data failover.

set live-data failover

Required Minimum Privilege Level: Advanced

Use this command to enable Live Data failover. This command automatically sets the system to run in duplex mode. Run this command on both Side A and Side B.

Command Syntax
set live-data failover

There are no required parameters.

unset live-data failover

Required Minimum Privilege Level: Advanced

Use this command to unset Live Data failover. This command automatically sets the system to run in simplex mode. Run this command on both Side A and Side B.

Command Syntax
unset live-data failover

There are no required parameters.

show live-data failover

Required Minimum Privilege Level: Ordinary

Use this command to display the Live Data cluster failover status and settings.

Command Syntax

show live-data failover

There are no parameters.

The command returns information on the Live Data server on which you run the command. The Live Data server information includes the current Live Data cluster settings, the status of the ActiveMQ connection, and the state of the cluster.

The possible cluster states are:

Cluster state	Description
PAIRED-ACTIVE	The cluster is in the active state and is communicating with the remote side.
PAIRED-STANDBY	The cluster is in the standby state and is communicating with the remote side.
ISOLATED-ACTIVE	The cluster is in the active state, but it is not communicating with the remote side.
ISOLATED-STANDBY	The cluster is in the standby state, but it is not communicating with the remote side.
SIMPLEXED-MODE	The cluster is working in simplex mode.
OUT-OF-SERVICE	The cluster is out of service.
CONNECTING	The cluster is attempting to do a handshake with the remote side.
TESTING	The cluster is unable to communicate with the remote side and is using the Test-Other-Side procedure to determine whether to become active or standby.

The console output after you run this command on the publisher side of a Live Data system is similar to the following:

```
admin:show live-data failover
# Failover settings..
Cluster failover enabled: true
Cluster ID: A
Remote side addr: not applicable for the publisher in auto-config
Auto config enabled: true

# ActiveMQ NetBridge..
Established

# Cluster state..
PAIRED-ACTIVE
```

Sample console output on the subscriber side is as follows:

```
admin:show live-data failover
# Failover settings..
Cluster failover enabled: true
```

```
Cluster ID: B
Remote side addr: cuic1
Auto config enabled: true

# ActiveMQ NetBridge..
Established

# Cluster state..
PAIRED-STANDBY
```

Live Data Syslog

Syslog servers and ports for the Live Data services are configured through the Unified Intelligence Center OAMP interface in the same way as the Unified Intelligence Center servers.



Note If Live Data Service goes down, an alert CUIC_LIVE_DATA_FEEDS_STOPPED is displayed in the RTMT counters (**Alert Central > Intelligence Center**). Use the failure details provided in the counters to troubleshoot the error scenario.

set live-data syslog-server

Required Minimum Privilege Level: Advanced

Use this command to set syslog configuration.

```
set live-data syslog-server syslogHostPrimary [syslogPortPrimary] [syslogHostSecondary
syslogPortSecondary]
syslogHostPrimary
```

Specifies the primary host (fully-qualified domain name or IP address) for syslog.

syslogPortPrimary

The syslogPortPrimary parameter is optional. Specifies the port for syslog. The default value is 514.

syslogHostSecondary

The syslogHostSecondary parameter is optional. Specifies the secondary host (fully-qualified domain name or IP address) for syslog.

syslogPortSecondary

The syslogPortSecondary parameter is optional. Specifies the port for syslog. The default value is 514.

unset live-data syslog-server

Required Minimum Privilege Level: Advanced

Use this command to unset syslog configuration.

unset live-data syslog-server syslogHostQualifier *{primarysecondaryall}*
primary

Unset the primary host information (fully-qualified domain name and port).

secondary

Unset the secondary host information (fully-qualified domain name and port).

all

Unset the primary and secondary host information (fully-qualified domain name and port).

show live-data syslog-server

Required Minimum Privilege Level: Ordinary

Use this command to show the current configuration for the Live Data syslog server.

show live-data syslog-server

There are no required parameters.

Monitor and Analyze System Performance Using Nmon

Nmon is a tool to monitor and analyze performance data. The following commands start and stop the nmon data collection.

utils live-data nmon start

Required Minimum Privilege Level: Advanced

Use this command to start the nmon capture.

Command Syntax

utils live-data nmon start *s* [*seconds*] *c* [*count*]

s

Specifies the time interval (1 to 60 seconds) between each collection.

c

Specifies the number of collections that you want to perform. Each collection requires about 1 Kilobyte of disk space.

utils live-data nmon stop

Required Minimum Privilege Level: Advanced

Use this command to stop the nmon capture. The data that you capture in this nmon session is saved in `nmon_output.nmon`.

Command Syntax
utils live-data nmon stop

There are no required parameters.

Live Data Socket.IO

Live Data Socket.IO pushes the Live Data to the Unified Intelligence Center Live Data reports. Socket.IO receives data from the Live Data JMS feed and pushes the data to subscribing clients.

show socketio status

Required Minimum Privilege Level: Ordinary

Use this command to show the Socket.IO service status.

show socketio status

There are no required parameters.

Socket.IO Service Attribute	Value
Server Status	<ul style="list-style-type: none"> • Active - The server is in service. • Not Active - The server is not in service. • Unavailable - The server is not available.
JMS Brokers	JMS brokers configured for the Socket.IO service.
Active Broker	<ul style="list-style-type: none"> • Local - The Socket.IO service is using the local JMS broker. • Remote - The Socket.IO service is using the remote JMS broker.
Client Count	The total number of clients currently connected to the Socket.IO service.
Polling Client Count	The number of polling clients.



Note If the server cannot establish a JMX connection, the server status is Unavailable. No other status is displayed. If the JMS Brokers, Active Broker, Client Count, or Polling Client Count are not available, the information related to that status does not display.

The console output is similar to the following:

```
Server Status: Active
JMS Brokers: tcp://localhost:61616,tcp://192.168.1.56:61616
Active Broker: Local
Client Count: 2001 (polling: 312)
```

Live Data SNMP

You can monitor the health of Cisco Live Data using an industry standard SNMP (Simple Network Management Protocol) network management station (NMS). The Live Data reporting engine exposes an SNMP Management Information Base (MIB): **CISCO-LIVEDATA-MIB**. This MIB supports instrumentation specifically for Cisco Live Data.

Because Cisco Live Data is co-resident with Unified intelligence Center, the Cisco Live Data SNMP agent integrates with the existing Unified intelligence Center agent infrastructure and uses the same Unified intelligence Center **sysObjectID**. You can use the existing Unified Intelligence Center user interfaces to configure the Live Data SNMP agent. The Unified intelligence Center primary agent uses and maintains the Live Data configuration.

The Live Data configuration includes MIB-II “system” MIB values; SNMP v1 or v2c community strings or SNMP v3 user names (with associated authentication and encryption protocols); and notification destinations (network management stations). See Configure SNMP-Associated Settings in the *Administration Console User Guide for Cisco Unified Intelligence Center* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html> for more details.

Live Data CISCO-LIVEDATA-MIB

The Live Data MIB, **CISCO-LIVEDATA-MIB** defines instrumentation unique to the Live Data servers (virtual machines). The instrumentation includes the following types of objects:

- **General Items** - attributes of the device and application.
- **Cluster Information** - cluster status and identity.
Cluster status is shared across all nodes of the cluster; cluster status is not device-specific unless there is only one node in the cluster.
- **Service Table** - service status and identity.
Exposed as a table.
- **Reporting Connection Table** - connection status and attributes (including metrics).
Exposed as a table.
- **Event Table** -
Exposed as a table and as SNMP notifications/traps.

Each of these tables is described in more detail below.



Note The MIB defines a single notification type; all nodes in all clusters may emit notifications.
The number of entries within each table may change over time, adapting to changes within the cluster.

Live Data MIB Textual Conventions

Table 76: Textual Conventions

Name	Syntax	Description
CldIndex	Unsigned32 (1..4294967295)	This syntax is used as the index into a table. A positive value identifies a unique entry in the table.
CldSeverity	INTEGER emergency(1), alert(2), critical(3), error(4), warning(5), notice(6), informational(7), debug(8)	This syntax is used to indicate the severity level of a notification or a logged event (or trace) message.

The severity levels are:

- **emergency**

Events of this severity indicate that a devastating failure occurred; the system or service is unusable. Immediate operator intervention is required.

- **alert**

Events of this severity indicate that a devastating failure is imminent that renders the system unusable. Immediate operator attention is necessary.

- **critical**

Events of this severity indicate that a service-impacting failure is likely to occur soon or an error occurred that the system did not handle appropriately. Operator attention is needed as soon as possible.

- **error**

Events of this severity contain important operational state information. The operational state information may indicate that the system experienced a temporary impairment or an error that the system handled appropriately. An operator should review the notification soon as possible to determine if more action is needed.

- **warning**

Events of this severity contain important operational state information that may be a precursor to an error occurrence. An operator should review the event soon to determine if more action is needed.

- **notice**

Events of this severity contain health or operational state information that may be pertinent to the health of the system. Administrator attention is not immediately required.

- **informational**

Events of this severity contain interesting system-level information that is valuable to an administrator in time, however, the event itself does not indicate a fault or an impairment condition.

- **debug**

Events of this severity provide supplemental information that may help diagnose or resolve a problem, but do not necessarily provide operational health status.

Live Data MIB General Objects

Table 77: General Objects

Object Name	Data Type	Description
cldServerName	SnmpAdminString	The server name object is the fully-qualified domain name of the Cisco Live Data server.
cldDescription	SnmpAdminString	The description object holds a textual description of the Cisco Live Data software installed on this server. The description is typically the full name of the application.
cldVersion	SnmpAdminString	The version object identifies the version number of the Cisco LiveData software that is installed on this server.
cldStartTime	DateAndTime	The start time object is the date and time that the Cisco LiveData software (the primary application service) was started on this server.
cldTimeZoneName	SnmpAdminString	The time zone name object specifies the textual name of the time zone where the Cisco LiveData server (host) is physically located.
cldTimeZoneOffset	Integer32	The time zone offset minutes object represents the number of minutes that the local time, in the time zone where the Cisco LiveData server (host) is physically located, differs from Greenwich Mean Time (GMT).
cldEventNotifEnable	TruthValue	The notification enable object allows a management station to disable, during run time, all outgoing Cisco LiveData notifications. During a maintenance window, the management station frequently stops, reconfigures, and restarts many application components which can generate periodic floods of notifications. Therefore, the management station typically disables the notifications during a maintenance window. This setting is persistent even after a restart of the agent. The management station must explicitly reset this object value back to 'true' to re-enable outgoing application notifications from this device.

Live Data MIB Cluster Information

Table 78: Cluster Information

Object Name	Data Type	Description
cldClusterID	SnmpAdminString	The cluster identifier (ID) object holds a cluster-unique textual identifier for this cluster (for example, 'sideA').

Object Name	Data Type	Description
cldClusterStatus	INTEGER: pairedActive(1), pairedStandby(2), isolatedActive(3), isolatedStandby(4), testing(5), outOfService(6)	<p>The cluster status object indicates the status of this cluster of Cisco Live Data servers. A cluster is a group of one or more Cisco Live Data servers. The cluster works cooperatively to consume and process inbound real-time data from one or more data sources. The primary node distributes work between worker nodes within the cluster. A cluster may have a peer cluster in a fault-tolerant deployment model that assumes data processing duties in the event where its active peer cluster fails.</p> <ul style="list-style-type: none"> • pairedActive The cluster is actively processing data and is communicating with its remote peer cluster. • pairedStandby The cluster is standing by (waiting to process data if necessary) and is communicating with its remote peer cluster. • isolatedActive The cluster is actively processing data but has lost peer-to-peer communication with its remote peer cluster. • isolatedStandby The cluster is standing by (waiting to process data if necessary) but has lost peer-to-peer communication with its remote peer cluster. • testing The cluster is unable to communicate with the remote peer cluster using the peer-to-peer connection. The cluster uses the 'test-other-side' procedure to determine whether to become active or go to a standby state. • outOfService The cluster is out of service.
cldClusterAddress	SnmpAdminString	<p>The cluster address object holds the hostname or the IP address of the remote peer cluster for peer-to-peer communication with the remote cluster.</p> <p>NOTE: On the Publisher node, the value of this object is N/A</p>

Live Data Service Table

Service Table Description

The service table is a list of Cisco Live Data dependent services. A service in this context is one or more executable processes that are configured to run on this server. Service table objects include both the service name and the current run state of that service. A single Live Data server has multiple running services, each of a different type, that encompasses the Live Data solution on a particular server. Some of these services work cooperatively with similar or dependent services on other server nodes in the cluster.

The SNMP agent constructs the service table at startup. The agent refreshes this table periodically during runtime to offer a near real-time status of configured services. The management station cannot add or delete service table entries. All objects in this table are read-only.

Service Entry Description

Each service entry represents a Cisco Live Data dependent service. The Live Data application software includes a collection of related services, each of which perform a specific, necessary function of the application.

Service Table Objects

Table 79: Service Table Objects

Object Name	Data Type	Description
cldServiceIndex	CldIndex	The service index is a value that uniquely identifies an entry in the services table. The SNMP agent arbitrarily assigns this value.

Object Name	Data Type	Description
cldServiceName	SnmpAdminString	The service name is a user-intuitive textual name for the Cisco Live Data dependent service. (Note: as shown in the VOS "utils service list" command.)
cldServiceState	INTEGER: 'unknown' (1), 'disabled' (2), 'starting' (3), 'started' (4), 'active' (5), 'stopping' (6), 'stopped' (7)	The service state is the last known state of the Cisco LiveData dependent service. The object value identifies the run status of a configured service installed on the Cisco LiveData server. <ul style="list-style-type: none"> • unknown The status of the service cannot be determined. • disabled An administrator has explicitly disabled the service. • starting The service is currently starting up, but has not yet completed its startup procedure. • started The service completed its startup procedure and is currently running. • active The service is started, is currently running, and is actively processing data. • stopping The service is stopping and is in the midst of its shutdown procedure. • stopped The service is stopped. The service is dysfunctional or impaired, or an administrator has explicitly stopped it.
cldServiceUpTime	DateAndTime	The up time object indicates the date and time that this service started.

Live Data Reporting Connection Table

Reporting Connection Table Description

The reporting connection table is a list of Cisco Live Data server reporting connections. A Live Data server maintains several active connections to data sources. Most often, these connections are contact center solution nodes that generate real-time data that is ultimately used for creating reports.

Reporting connection table objects include objects that identify the reporting connection, the current state of that connection and a set of metrics and attributes that indicate connection health and performance. A single Live Data server has multiple reporting connections, each to a different peer node and to multiple data sources from a single node. The SNMP agent constructs the reporting connection table at startup. The agent refreshes this table periodically during runtime when each Live Data service reports connection states.

The management station cannot add or delete reporting connection table entries from the table. All objects in this table are read-only.

Reporting Connection Entry Description

Each reporting connection entry represents a Cisco Live Data reporting connection. The Live Data application connects to a number of data sources, each of which sends real-time data as a stream to the Live Data server.

Reporting Connection Objects

Table 80: Reporting Connection Objects

Object Name	Data Type	Description
cldRptConnIndex	CldIndex	The reporting connection index is a value that uniquely identifies an entry in the reporting connection table. The SNMP agent arbitrarily assigns this value.
cldRptConnServerID	SnmpAdminString	The reporting connection server identifier (ID) is a user-intuitive textual identification for the Cisco LiveData connection. This identifier is indicative of the source of the real-time data streamed using this reporting connection.
cldRptConnServerAddress	SnmpAdminString	The reporting connection server address object holds the hostname or IP address of the peer node in this reporting connection.
cldRptConnState	INTEGER: 'inactive' (1) 'active' (2)	The reporting connection state object indicates the current state of this reporting connection. The state is either active or inactive.
cldRptConnStateTime	DateAndTime	The reporting connection state time object records the date and time that this reporting connection transitioned into its current state.
cldRptConnEventRate	Gauge32	The reporting connection event rate indicates the number of events that arrive using this connection per second.
cldRptConnHeartbeatRTT	Gauge32	The reporting connection heartbeat round-trip time object indicates the time, in milliseconds, for heartbeat requests to return from the peer node in this reporting connection.
cldRptConnSocketConnects	Counter32	The reporting connection socket connects object counts the number of successful socket connections made to the peer node in this reporting connection.
cldRptConnSocketDisconnects	Counter32	The reporting connection socket disconnects object counts the number of socket disconnects with the peer node in this reporting connection. This object is used with cldConnSocketConnects to identify unstable connections to a particular endpoint.
cldRptConnMessagesDiscarded	Counter32	The reporting connection messages discarded object counts the number of discarded messages that the peer node sent in this reporting connection.
cldRptConnDSCP	Integer32	The reporting connection DSCP (Differentiated Services Code Point) object holds the Differentiated Services (DS) value currently used by this connection for Quality of Service (QoS) marking.

Live Data Event Table

Event Table Description

The event table is a list of active Cisco Live Data events. The SNMP agent constructs the event table at startup and it fills the table as 'raise' state events are generated. Events with the same cldEventID value overwrite existing events in the table with the same EventID (in other words, only the most recent events persist). The management station cannot add or delete event table entries from the table. All objects in this table are read-only.

Event Entry Description

Each event entry represents a Cisco Live Data event. The Live Data application software generates events when an unusual condition occurs that potentially affects the functioning of the Cisco Live Data server.

Event Table Objects

Table 81: Event Table Objects

Object Name	Data Type	Description
cldEventIndex	'CldIndex' TEXTUAL-CONVENTION	The event index is a value that uniquely identifies an entry in the event table. The SNMP agent arbitrarily assigns this value.
cldEventID	Unsigned32	The event identifier (ID) object is the unique notification message identifier that the Live Data server assigns. This identifier is unique for each different notification but consistent for each instance of the same notification. Use this id to correlate 'clear' state notifications to 'raise' state notifications.
cldEventAppName	SnmpAdminString	The event application name object specifies the service-specific name of the functional service that generated this notification.
cldEventName	SnmpAdminString	The event name object specifies the service-specific name of the LiveData notification message. The object value is used to group and correlate similar notifications.
cldEventState	INTEGER: 'raise' (1), 'clear' (2)	The event state object identifies the state (not severity) of the notification and potentially the status of the functional component that generated the notification. The possible states are: <ul style="list-style-type: none"> • raise : A raise state identifies a notification received as a result of a health-impacting condition, such as a process failure. A subsequent clear state notification follows when the error condition is resolved. A node which generates a 'raise' state event may be impaired and likely requires an administrator's attention. • clear : The clear state indicates that the condition which generated a previous raise notification is resolved. This state may occur automatically with fault-tolerant deployments or may occur when an administrator intervenes.
cldEventSeverity	'CldSeverity' TEXTUAL-CONVENTION	The event severity object indicates the severity level of this notification.
cldEventTimestamp	DateAndTime	The event time stamp object specifies the date and time that the notification was generated on the originating device.

Object Name	Data Type	Description
cldEventText	SnmpAdminString	The event text is the full text of the notification. This text includes a description of the generated event, component state information, and potentially a brief description of administrative action that may be necessary to correct the condition that caused the event to occur.

Live Data MIB Notifications

Notification Type

cldEventNotif

Description

This notification describes an unusual condition that occurred that can potentially affect the functioning of the Cisco Live Data server. A functional service of the Cisco Live Data server sends a notification. The notification type provides operational state information about the service generating the notification at the time such service-impacting conditions occur.

Notification Type Objects

Object Name	Description
cldEventID	The unique event message identifier that the Live Data server assigns.
cldServerName	The host name or the fully qualified domain name of the Live Data server from which this event originated.
cldEventAppName	The service-specific name of the functional service that generated this notification.
cldEventName	The service-specific name of the Live Data notification message.
cldEventState	The state of the notification, either 'raise' or 'clear'.
cldEventSeverity	The severity level of this notification.
cldEventTimestamp	The date and time that the notification was generated.
cldEventText	The full text of the notification.

Live Data SNMP Event Correlation

The CISCO-LIVEDATA-MIB notification type (cldEventNotif) defines a set of objects that are contained within a Live Data SNMP notification. Live Data notifications are "stateful." A "raise" state event indicates a problem and a "clear" state event follows when the problem resolves or after the component engages fault-tolerance mechanisms to self-heal. To maintain an accurate state at the network management station, you can write rules to automatically correlate "clear" state events to existing "raise" state events and acknowledge those notifications at the management station.

The following notification type objects are used for event correlation.

Table 82: Live Data Notification Type Objects

Object Name	Description
cldEventID	The unique numeric event message identifier for this event.
cldServerName	The fully-qualified domain name of the Cisco Live Data server that generated the notification.
cldEventAppName	The name of the Cisco Live Data functional service that generated this event.
cldEventName	The service-specific name of the Cisco LiveData event message.
cldEventState	The state of the event, either 'raise' or 'clear'. A 'raise' state event generates when an unusual or service-impacting condition occurs. A 'clear' state event generates when a prior condition is resolved.

Live Data events are numerically identified in ascending order where "raise" state events have an odd value and "clear" state events have an even value. If a "raise" state event has a matching "clear" state event, the "clear" state event has the next (higher) even value. "Single-state raise" events are "raise" state events with no matching "clear" state event. A "single-state raise" event is an error condition that typically requires manual intervention to resolve.

To match "clear" state events to existing "raise" state events, match the object cldServerName (from the same device), cldEventAppName (from the same application), and cldEventName (the same event group) value from each event. In many cases, "clear" state events map to "raise" state events. The matching "raise" state event is that event with an even valued EventID that is less than the EventID value of the "clear" state event (for example, 202 is matched to 201). There may be more than one "raise" state event associated with that "clear" state event. The "clear" state event correlates with all existing "raise" state events with the matching ServerName, EventAppName and EventName. For example, assume that the "raise" state events #301 and #303 generate, followed by the "clear" state event #304. In this case, #304 correlates to both #301 and #303, acknowledging both "raise" state events.

To understand the relationship between certain "raise and "clear" state events, see the table of Live Data events and use the "See Also" field to relate events. Each event has a textual label to identify and relate each event in the table.

Events may have certain parameters associated with the event, such as a server IP address or a service state. These parameters are expressed as "tags" within the message text. A "tag" is a name/value pair surrounded by brackets, for example: [server_address=192.168.0.1]. The parameters are expressed this way to facilitate easier (automated) parsing of event text. Because the parameters are generalized across the full set of events, a separate table describes the parameters with labels associated for easy cross-referencing of an event with the parameters used.

Live Data SNMP Parameters

This table summarizes the parameters passed into the Live Data SNMP notifications.

Table 83: Live Data SNMP Parameters

Parameter ID	Tag	Description
PARAM_JMS_URL	jms_url	URL under which JMS server is located.

Parameter ID	Tag	Description
PARAM_JMS_SUBJECT	jms_subject	Topic, or queue, about which a JMS publication is issued.
PARAM_JMS_MESSAGE	jms_message	Message (typically JSON encoded) to/from JMS broker (ActiveMQ).
PARAM_AGENT_ID	agent_id	CCE agent identifier.
PARAM_TIP_MESSAGE	tip_message_class	CCE to Live Data (TIP) message class.
PARAM_TIP_CLIENT_SEQUENCE_GROUP	tip_client_seqgrp	TIP Client Sequence Group; Live Data, low-level protocol, current group sequence number.
PARAM_TIP_SERVER_SEQUENCE_GROUP	tip_client_seqgrp	TIP Client Sequence Group; Live Data, low-level protocol, current group sequence number.
PARAM_TIP_CLIENT_SEQUENCE_NUMBER	tip_client_app_seqnum	CCE, application level, current message sequence number.
PARAM_TIP_CLIENT_APP_SEQUENCE_NUMBER	tip_server_app_seqnum	Live Data, application level, current message sequence number.
PARAM_TIP_SERVER_APP_SEQUENCE_NUMBER	tip_server_app_seqnum	CCE, application level, current message sequence number.
PARAM_ERROR_DESC	message_error	Description of error associated with encoding/decoding/processing of CCE to Live Data protocol message.
PARAM_PERIPHERAL_ID	peripheral_id	CCE peripheral ID.
PARAM_SERVER_ID	server_id	Unique identifier to server or service id in CCE (example: PG) or Live Data (example: Router Spout).
PARAM_CONNECTION_USAGE	connection_usage	Defines to which protocol, or purpose, a given connection is associated with (TOS, TIP, and so on).
PARAM_SERVER_ADDRESS	server_address	IP or hostname to a server to which Live Data is a client (example: PG).
PARAM_SERVER_URL	server_url	URL to a server to which Live Data is a client (example: ActiveMQ).
PARAM_SERVER_PORT	server_port	IP port to connect to a server to which Live Data is a client (example: PG).
PARAM_SERVER_USERNAME	server_username	Username for accessing a given server.
PARAM_DATABASE_NAME	database_name	Database name.
PARAM_OPERATION_TYPE	operation_type	Description of an operation type (example: start, stop, disable, enable, and so on).
PARAM_OPERATION_ERROR_DESC	operation_error_desc	Error description associated with a given operation failure
PARAM_CONFIGURED_LIMIT	limit	Limit (maximum, or minimum) to a given configuration element.
PARAM_CONFIGURED_PROPERTIES	properties	Configuration properties and current values.
PARAM_DATABASE_OBJECT_TYPE	db_object_type	Database object as represented in-memory.

Parameter ID	Tag	Description
PARAM_DATABASE_OBJECT_ID	db_object_id	Database object id (typically unique key).
PARAM_DATABASE_VERSION_EXPECTED	db_ver_expected	Expected database schema version.
PARAM_DATABASE_VERSION_READ	db_ver_read	Database schema version retrieved from DB.
PARAM_JMX_MBEAN_NAME	jmx_mbean_name	JMX bean name.
PARAM_STATE	state	State description of a given object (example: State Machine state transition).
PARAM_PRIOR_STATE	prior_state	Prior state of a given object (example: connection state).
PARAM_TIP_SIDE	tip_server_side	CCE server side to which Live Data is associated (example: side A or side B).
PARAM_HEARTBEAT_MISSED_COUNT	missed_heartbeats	Currently missed heartbeats during communication CCE to Live Data.
PARAM_TIME_CHANGE	tip_time_change	CCE time server adjustment in milliseconds.
PARAM_CONNECTION_STATISTICS	connection_stats	CCE to Live Data connection statistics.
PARAM_AGENT_TEAM_ID	agent_team_id	CCE Agent Team Identifier.
PARAM_MRD_ID	mrd_id	CCE Media Router Domain Identifier.
PARAM_DESCR_GENERIC	descr	Generic Description field.
PARAM_ZOOKEEPER_ZNODE	znode	Zookeeper znode name.
PARAM_VALUE	value	Value associated with a given parameter.
PARAM_INPUT	input	Input value.
PARAM_CURRENT_STATE	current_state	Current state of a given object (example: connection state).
PARAM_NEW_STATE	new_state	New state of a given object (example: connection state).
PARAM_SEQ_NUM	seqnum	Message Sequence Number.
PARAM_MESSAGE	message	Actual message in text format.
PARAM_LATENCY	latency	Latency time.
PARAM_LAST_VIRTUAL_TIMESTAMP	last_vtimestamp	Last virtual time stamp (used for Live Data cluster messaging).
PARAM_NEW_VIRTUAL_TIMESTAMP	new_vtimestamp	New virtual time stamp (used for Live Data cluster messaging).



CHAPTER 13

Cisco Identity Service Serviceability

- [Cisco Identity Service Logs, on page 307](#)
- [Set up a Remote Syslog Server, on page 308](#)

Cisco Identity Service Logs

The Cisco Identity Service generates logs, which you can view in the Real Time Monitoring Tool.

You set the level of logging you want by using Cisco Identity Service Management.

Set the Cisco Identity Service Log Levels

You set log levels for the Cisco Identity Service using Cisco Identity Service Management.

Procedure

- Step 1** In Unified CCE Administration, navigate to **System > Single Sign-On**.
 - Step 2** Click **Identity Service Management**.
The Identity Service Management window opens.
 - Step 3** Enter your user name, and then click **Next**.
 - Step 4** Enter your password, and then click **Sign In**.
The Cisco Identity Service Management page opens, showing the **Nodes**, **Settings**, and **Clients** icons in the left pane.
 - Step 5** Click **Settings**.
 - Step 6** From the **Settings** page, click **Troubleshooting**.
 - Step 7** Set the local log level by choosing from **Error**, **Warning**, **Info** (the default), **Debug**, or **Trace**.
 - Step 8** Click **Save**.
-

Set up a Remote Syslog Server

To help in troubleshooting, you can identify a remote Syslog server as a repository for receiving errors in Syslog format.

Procedure

- Step 1** In Unified CCE Administration, navigate to **System > Single Sign-On**.
- Step 2** Click **Identity Service Management**.
The Identity Service Management window opens.
- Step 3** Enter your user name, and then click **Next**.
- Step 4** Enter your password, and then click **Sign In**.
The Cisco Identity Service Management page opens, showing the **Nodes**, **Settings**, and **Clients** icons in the left pane.
- Step 5** Click **Settings**.
- Step 6** From the **Settings** page, click **Troubleshooting**.
- Step 7** To receive errors in Syslog format, enter the name of the Remote Syslog Server in the **Host (Optional)** field.
- Step 8** Click **Save**.

Note The remote syslog server setting applies across the cluster.



CHAPTER 14

CCE Serviceability and Monitoring using AppDynamics

- [Overview, on page 309](#)
- [Supported Applications, on page 309](#)
- [Prerequisites, on page 311](#)
- [Performance Monitoring, on page 312](#)
- [Dashboards , on page 319](#)
- [Check Logs, on page 323](#)
- [Things to Know, on page 325](#)

Overview

For Cisco Contact Center Enterprise solution, it is important to have continuous and seamless monitoring of the deployed solution, and automated alerting when anomalies are detected. AppDynamics provides a solution for application and platform performance monitoring that helps to achieve the following:

- Platform, application, and end user monitoring (EUM) through dashboards and metrics
- Automated alerting mechanism in case of anomaly detection

For ordering and setting up AppDynamics SAAS controller, License key, and Beacon URL please contact appd_ucce_sales@cisco.com



Note For AppDynamics, CCE supports SaaS and On-Prem controller (version 21.4.10-24683) over secure connection only.

Supported Applications

All CCE solution components are supported except ECE, Customer Collaboration Platform (CCP), and Cloud Connect server. Here is a table depicting what is instrumented in each component and monitored:

SI No	Component Name	Machine Agent (Server Visibility)	.Net Agent (For Windows Perfmon Integration)	JVM App Agents
1	Finesse Note End-user monitoring is supported for Finesse.	✓	Not Applicable	• Finesse-Desktop
2	CUIC	✓	Not Applicable	CUIC-Reporting
3	LiveData	✓	Not Applicable	• LiveData-ActiveMQ • LiveData-SocketIO
4	IdS	✓	Not Applicable	IdS Tomcat
5	VVB	✓	Not Applicable	• Speech-Server • VVB-Engine
6	CVP OAMP	✓	Not Applicable	OAMP
7	CVP ReportingServer	✓	Not Applicable	• ReportingServer • WebServicesManager
8	CVP Call/VXMLServer	✓	Not Applicable	• CallServer • VXMLServer • WebServicesManager
9	Router	✓	✓	Not Applicable
10	Logger	✓	✓	Not Applicable
11	PG	✓	✓	CCEJGW
12	AW-HDS	✓	✓	CCEAdmin
13	AW-HDS-DDS	✓	✓	CCEAdmin

**Note**

- CCESERVERAGENT JVM is an extension of machine agent for ICM nodes. Each ICM node will have one CCESERVERAGENT instance mapped to it.
- CCESERVERAGENT is not used for application performance monitoring. It is used only for mapping the windows server to the application in AppDynamics controller.
- LiveData-Worker JVM App Agent is disabled by default. You can enable it using the **set live-data appd-monitoring enable** CLI. For more information on the CLI, see the *Live Data CLI Commands* section in the [Cisco Unified Contact Center Enterprise Installation and Upgrade Guide](#).

Prerequisites

Application Group and Agent Licenses

Before the applications can be configured for performance monitoring, ensure that an AppDynamics application group is created and the required number of agent licenses are procured and allocated. An access key is generated for the application group. This access key is required later during the configuration procedure.

For details on how to acquire agent licenses, please contact appd_ucce_sales@cisco.com and for details on application group, access keys etc., see the documentation on AppDynamics at: <https://docs.appdynamics.com/display/PRO45/AppDynamics+Essentials>.

**Note**

For end user monitoring on Finesse, you must procure AppDynamics ENUM license.

Cloud Connect

The CLI commands described in this chapter must be run from the Cloud Connect server. The nodes on which performance monitoring has to be enabled must be part of the Cloud Connect server orchestration inventory.

For installing and configuring Cloud Connect, refer to the *Install Cloud Connect* section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at

<https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html>.

If Cloud Connect is on 12.6(2) and the target Windows and VOS nodes are on 12.6(1) during stagewise upgrade, ensure below ESs and COP are applied in respective 12.6(1) target nodes:

Component	ES/COP
Unified ICM	ES67
Unified CVP	ES19

Component	ES/COP
Finesse	ucos.appDynamicsProxyUpdate.1261.cop.sgn
Cisco Unified Intelligence Center	ucos.appDynamicsProxyUpdate.1261_rollback.cop.sgn
Live Data	
Cisco Identity Service	
Cisco Virtualized Voice Browser	

AppDynamics performance monitoring are supported in the following deployment types:

- UCCE-2000-Agents
- UCCE-4000-Agents
- UCCE-12000-Agents
- UCCE-24000-Agents
- PCCE-2000-Agents
- PCCE-4000-Agents
- PCCE-12000-Agents



Note The UCCE-12000-Agents, UCCE-24000-Agents, and PCCE-12000-Agents deployment types are supported only for AppDynamics performance monitoring and not for orchestration.

For information about how to onboard nodes to Cloud Connect server, refer to the **Orchestration Deployment Task Flow** section in the *Unified CCE or Packaged CCE Install and Upgrade Guide*.

CCE Solution Components

The CCE solution components existing in domain should have a unique FQDN. The components existing in a workgroup should have a unique hostname to register with AppDynamics controller for performance monitoring.

Performance Monitoring

In order to monitor the performance of CCE applications, platforms, and end-user-facing application such as Finesse desktop using AppDynamics, an administrator must configure and enable performance monitoring on target node.



Note Parallel execution of same or different CLI for AppDynamics on Cloud Connect server is not allowed.



Note If Cloud Connect is on 12.6(2), you can enable or check the status of performance monitoring or test the connection with AppDynamics controller only after upgrading the target node to 12.6(2). However, you can disable performance monitoring if the target node is on 12.6(1).



Note Before upgrading the Distributor node from 12.6(1) to 12.6(2), disable AppDynamics performance monitoring on 12.6(1) and re-enable it after upgrading to 12.6(2). If AppDynamics performance monitoring is not disabled before the Distributor node is upgraded to 12.6(2), then post upgrade, restart the Distributor node.

Enable Performance Monitoring

To enable performance monitoring on Windows or VOS nodes, run the **utils app-monitoring enable** command. You can select a single node or a group of nodes from either Cloud Connect publisher or subscriber to enable performance monitoring. Ensure that the number of selected nodes doesn't exceed 10. Provide the details for configuring these nodes for monitoring. Deployment Name configured in Orchestration inventory is used as the application name in AppDynamics. For more information, see the **Add Deployment Type and Deployment Name** section in the Orchestration chapter of *Unified CCE or Packaged CCE Install and Upgrade Guide*.

Performance monitoring is enabled only after restarting the target node. If you choose not to restart the servers immediately, manually restart them later for the changes to take effect.

All the supported AppDynamics agents on the target nodes are enabled for monitoring; the administrator can't control the enable or disable of a specific AppDynamics agent on the target node.



Note You can also use this command to update any existing configuration details on selected nodes.

Command	utils app-monitoring enable
Description	This command enables performance monitoring on selected nodes.

Expected Inputs	
------------------------	--

Select the node on which you need to enable performance monitoring and provide the following information:

- Note** You can select a single node or a group of nodes from either Cloud Connect publisher or subscriber to enable performance monitoring. Ensure that the number of selected nodes doesn't exceed 10.
- **Controller Host:** The hostname/URL of the AppDynamics Controller. Agents may connect directly to the Controller or through a proxy.
 - **Controller Port:** The port on which the AppDynamics Controller listens for agent traffic.
 - **Account Name:** The name of the account listed in the AppDynamics Controller. A single tenant Controller has two accounts: a default account name and an internal system account. For most connections, use the default account name.
 - **Account Access Key:** A unique key associated with the AppDynamics Controller account. This is used as the API token by agents to authenticate/authorize themselves with the Controller.
 - **Beacon URL:** The service endpoint where Javascript agents will connect for sending the end user monitoring metrics.
 - **Beacon Access Key:** The access key used by Javascript agents for authenticating or authorizing themselves with the Beacon server. This is different from the Account Access Key mentioned above.
 - **Proxy Host:** Proxy server IP/hostname via which the AppDynamics controller is connected.
 - **Proxy Port:** Proxy port for connecting to the proxy server.
 - **Username:** Username of the AppDynamics controller account.
 - **Password:** Password of the AppDynamics controller account.

Note Username and Password are used for enabling Windows Event monitoring on ICM nodes. The administrator has an option to confirm on whether AppDynamics Windows event monitoring must be enabled or not, when the ICM node is selected for enabling AppDynamics. The Username and Password will be requested only when the administrator confirms to enable Windows Event Monitoring on ICM nodes.

Note Proxy Host and Proxy Port will be requested only when the administrator confirms to use proxy for application monitoring. Using proxy for application monitoring is optional.

	<p>Note Beacon URL and Beacon Access Key used for end-user monitoring are applicable only for Finesse node. For more information on how to generate a Beacon Access Key, refer to the Generate a Beacon Access Key section below:</p> <p>Confirm to proceed, and select the option to restart.</p>
Expected Outcome	Performance monitoring is configured for all the selected nodes and enabled if restart option is selected as "Yes". Windows Event Monitoring is enabled for ICM nodes based on administrator's confirmation. Proxy is configured for application monitoring based on administrator's confirmation to use proxy for application monitoring.



Note Application monitoring configuration on Unified ICM and Unified CVP will be removed as part of Unified ICM 12.6(2) or Unified CVP 12.6(2) uninstall only when you upgrade from 12.5(x). If application monitoring is already enabled and if you want to uninstall and reinstall Unified ICM 12.6(2) or Unified CVP 12.6(2) software, after the reinstallation, reconfigure application performance monitoring using the **utils app-monitoring enable** CLI.



Note If performance monitoring is already enabled, and if you want to add or delete the component in Unified ICM, then follow the below steps to update the performance counters for monitoring.

- Disable application performance monitoring using the **utils app-monitoring disable** command.
- Add or delete the component in the Unified ICM.
- Enable application performance monitoring using the **utils app-monitoring enable** command.

When application performance monitoring is enabled, the system specific and CCE-specific performance counters are enabled by default. You can add more counters for deployment by editing the **.NET Agent config file**. Refer to <https://docs.appdynamics.com/display/PRO21/Configure+the+.NET+Agent>. If you are adding more counters, ensure that you don't exceed 200 counters on a virtual machine. Manually added counters will be reset to the default value if you disable or enable application performance monitoring. The counters added to the monitoring list includes all the installed CCE services including the disabled services. Hence, delete the disabled CCE services from the server if they are not required.



Note Performance monitoring starts on VOS components approximately 15 to 20 minutes after reboot. During this period, performance monitoring status for the target node in **utils app-monitoring status** CLI will be shown as Disabled.

Generate Beacon Access Key

Perform the following steps to generate the Beacon Access Key:

1. Log in to AppDynamics controller.
2. Click **User Experience** tab.
3. Click **Add App** in Browser Apps tab.
4. Select Create an application using the Getting Started Wizard, and press **OK**. The Set Browser Application section appears.
5. Enter the application name in the Set Browser Application section. Click **Continue**. The Beacon Access Key will be generated.
6. The Send and Verify a Test Page operation will be initiated, and it might take up to two minutes to complete. Once the activity is completed, the message, Beacon Sent and Data Received & Page Created is displayed with a tick mark.
7. Then, the message, You have successfully verified the configuration is displayed with a tick mark in the Instrument your own web pages section. Click **Continue**, and click **Save** in the next page.
8. Click on the **User Experience** tab to verify if the browser application has been created with the newly generated Beacon access key.

Update Performance Monitoring Configuration

To update the configuration details for performance monitoring, run the **app-monitoring enable** command. You must restart the servers for the changes to take effect. For details on the command, see [Enable Performance Monitoring, on page 313](#).

Disable Performance Monitoring

To disable performance monitoring on Windows and VOS nodes, run the **app-monitoring disable** command. Performance monitoring will be disabled after restart of target node. The configurations will, however, be retained. Administrator will not be allowed to disable any specific AppDynamics agent on the target node. All supported AppDynamics agents will be disabled by default.

Command	utils app-monitoring disable
Description	This command is used to disable performance monitoring on selected nodes.
Expected Inputs	Select the node on which performance monitoring needs to be disabled. Confirm to proceed.
Expected Outcome	Performance monitoring is disabled for all the selected nodes.



Note If the Cloud Connect is on 12.6(2), you can enable or disable AppDynamics only after upgrading the target node to 12.6(2).

Check Status of Performance Monitoring

To check whether performance monitoring is enabled, disabled, or just configured but not enabled, on selected Windows or VOS nodes, run the **utils app-monitoring status** command.

Command	utils app-monitoring status
Description	This command is used to check if performance monitoring is enabled on selected nodes. This command also shows the following: <ul style="list-style-type: none"> • Proxy enabled status • Windows Event monitoring enabled status for ICM nodes
Expected Inputs	Select the node for which you want to check the status, and confirm to proceed.
Expected Outcome	Shows whether the configuration details for performance monitoring is enabled, disabled, or updated for the selected nodes: <ul style="list-style-type: none"> • If an update is made to the existing configuration and the node is restarted, then the status shows the updated configuration as current configuration used by AppDynamics performance monitoring. • If an update is made to the existing configuration and the node is not restarted, then the status shows both the current configuration used by AppDynamics performance monitoring as well as the to-be-applied configuration which will be applied post restart.

Test Connection with AppDynamics Controller

To test whether the configured Windows and VOS nodes are able to connect to the AppDynamics controller, run the **utils app-monitoring test-connection** command.

Command	utils app-monitoring test-connection
Description	This command is used to test the connectivity of selected Windows or VOS nodes to the AppDynamics controller.
Expected Inputs	Select the nodes for which you want to test the connectivity status.
Expected Outcome	Shows whether the selected nodes are able to connect to the AppDynamics controller.

Configure Thresholds and Alerts for Monitoring

We recommend using the templates delivered for configuring threshold and alerts on the AppDynamics controller.

- The Cisco-delivered templates can be imported on the application. For details on managing templates, see <https://docs.appdynamics.com/display/PRO21/Configure+and+Manage+Alerting+Templates>. For

downloading template, see [https://software.cisco.com/download/home/268439622/type/283914286/release/12.6\(1\)](https://software.cisco.com/download/home/268439622/type/283914286/release/12.6(1))

- Once the template is imported, you have to replace the default email address (support@cisco.com) with a valid email address for alert notification.
- Adding at least one valid email address is mandatory. However, you can add multiple email addresses.
- Threshold for alerts is enabled by default as part of Cisco-delivered template.



Note You can also view, create, overwrite, delete, export, apply and disable the template on the application. For details on managing templates, see <https://docs.appdynamics.com/display/PRO21/Configure+and+Manage+Alerting+Templates>.

Configure JMX Monitoring and Alerting Templates for Finesse Desktop

We recommend using the following templates to configure JMX Monitoring for Finesse Desktop.

- Finesse_JMX_Metrics_Configuration.xml
- Finesse_JMX_Metrics_AlertingTemplate.json

Follow these steps to import the templates to the respective application:

1. Navigate to the respective application on the AppDynamics controller.
2. Select Tiers & Nodes section menu.
3. From the **Finesse-Desktop** tier, select the Finesse node.
4. Select the **JMX** tab.
5. Click the **Configure JMX Metrics** icon.
6. Click the **Import** icon.
7. Click the **Choose File** button.
8. Select the **Finesse_JMX_Metrics_Configuration.xml** file.
9. Click the **Import** button. The **FinesseMetrics List** is displayed if the import succeeds.
10. Import **Finesse_JMX_Metrics_AlertingTemplate.json**. See [Configure Thresholds and Alerts for Monitoring, on page 318](#) for more information on importing the alerting template.

Dashboards

Dashboards are used to display the health of the system in a graphical manner on the AppDynamics controller. Data such as CPU and memory usage are collected from the system at platform level. Data such as health status of Java agents and .NET agents are collected from the system at application level. Administrators can

build custom dashboards with various widgets to visualize the data from individual systems as well as all the systems in the deployment. These dashboards can be imported or exported when deploying new CCE tenants.

For more information on Dashboards, see <https://docs.appdynamics.com/display/PRO45/Dashboards+and+Reports>.

Create Dashboards Using Templates

Administrators can create new dashboards or edit the dashboard template (JSON file) provided by us. This edited template file can then be imported to the AppDynamics Controller via the **Dashboards & Reports** tab.

For downloading template, see [https://software.cisco.com/download/home/268439622/type/283914286/release/12.6\(2\)](https://software.cisco.com/download/home/268439622/type/283914286/release/12.6(2)).

Edit the following strings in the template:

- "name" - Provide an appropriate name, which is displayed as the dashboard name in the Controller. For example, "Arihant - 2K Dashboard".
- "applicationName" - Update this with the corresponding application name for which you want to create a dashboard.



Note If WidgetName is "EventListWidget", then don't change the "applicationName".

- "entityName" - Set the name of the system that is monitored.
 - If the "entityType" is set to "APPLICATION_COMPONENT_NODE", update this string with the corresponding AW component node name. For example, "UCCEAWHDS121A".

Once the template file is edited and imported, the dashboard will display the performance and health status of the system.



-
- Note**
- If the "entityType" is set to "APPLICATION_COMPONENT", then do not make any changes to the "entityName".
 - If the "entityType" is set to "BUSINESS_TRANSACTION", do not make any changes to the "scopingEntityName".
 - There are no changes required in these cases as the type of entity is a tier-name, which is common to all the nodes in an application.
-

End User Monitoring

End user monitoring is available for the Finesse desktop application. It provides various browser-based metrics, such as the most frequently used browser, the most commonly used browser version, etc. It can provide geographical location of a Finesse agent desktop. The AppDynamics agents in the browser sends the metrics

to the AppDynamics Controller. You can view these metrics in the **User Experience** tab of the AppDynamics Controller application.

When you run the **app-monitoring enable** command to enable performance monitoring for Finesse, end user monitoring is also enabled. There is no additional step required. The Beacon URL and the Beacon Access Key that you provided when running the command are saved in the Finesse server. The network connectivity between the Finesse Agent desktop browser and the Beacon host, however, must be available. The Beacon host must be on the allowed list in the proxy server.

For more information, see <https://docs.appdynamics.com/display/PRO45/End+User+Monitoring>.

View Metrics

Once the monitoring is enabled on the VOS and Windows nodes, the AppDynamics agents start sending out performance metrics to the AppDynamics controller. These monitored metrics, also known as counters, are shipped from the Windows machines as performance counters, and from the respective JVMs of the VOS machines as JMX counters. These metrics can be viewed on the AppDynamics Controller interface and later utilized for setting thresholds, alerts, etc.

JMX Counter Thresholds

Cisco Finesse provides important JMX counters with associated threshold values that can be used to monitor the health of Finesse. The following tables list the JMX counters with corresponding threshold values at the login phase and steady phase.



Note The JMX counter IntervalLoginOperations with the JMX object name `com.cisco.ccbu:category=LoginStats,component0=LoginStats-webservices` will be used to determine the total number of logins.

If the number of logins that happened in the last 15 seconds is greater than 5, then it is login phase. Else it is steady phase. Respective threshold will be used dynamically based on the number of logins.

Table 84: JMX Counters on Tomcat Processes (Port 12399) - Login Phase Thresholds

JMX Counter	Description	JMX Object Name	Threshold at Login Phase
ThreadCount	The number of threads running at the current moment.	java.lang:type = Threading	400
PeakThreadCount	The maximum number of threads run at the same time since the JVM was started or the peak was reset.	java.lang:type = Threading	500
currentThreadCount	The number of threads the thread pool currently has (both busy and free).	Catalina:type = ThreadPool, name = "http-apr-127.0.0.1-8082"	120

JMX Counter	Description	JMX Object Name	Threshold at Login Phase
currentThreadsBusy	The number of threads currently processing requests.	Catalina:type = ThreadPool, name = "http-apr-127.0.0.1-8082"	100
RequestLongestTime	The maximum amount of time taken to complete an API request, in milliseconds.	com.cisco.ccbu:category = WebAppStats, component0 = AggregateWebappStats	4000
processCPULoad	The CPU load in this process.	java.lang:type = OperatingSystem	0.6
NumOfActiveAgentsLoggedIn	The number of agents logged in with XMPP Presence as available in the current side.	com.cisco.ccbu:category = AWSSubsystem, component0 = AWS Statistics Counter	1500
NumOfAgentsLoggedIn	The number of agents and supervisors logged in currently.	com.cisco.ccbu:category = AWSSubsystem, component0 = AWS Statistics Counter	2010

Table 85: JMX Counters on Tomcat Processes (Port 12399) - Steady Phase Thresholds

JMX Counter	Description	JMX Object Name	Threshold at Steady Phase
ThreadCount	The number of threads running at the current moment.	java.lang:type = Threading	400
PeakThreadCount	The maximum number of threads run at the same time since the JVM was started or the peak was reset.	java.lang:type = Threading	500
TotalCallsInSystem	The total number of active calls in the system.	com.cisco.ccbu:category = AWSSubsystem, component0 = AWS Statistics Counter	1400
AverageProcessingTime	The average time taken for processing CTI messages, in milliseconds.	com.cisco.ccbu:category = AWSSubsystem, component0 = CTIMessage Statistics Counter	20 ms
currentThreadCount	The number of threads the thread pool currently has (both busy and free).	Catalina:type = ThreadPool, name = "http-apr-127.0.0.1-8082"	120
currentThreadsBusy	The number of threads currently processing requests.	Catalina:type = ThreadPool, name = "http-apr-127.0.0.1-8082"	20
RunnablesQueued	Runnables (CTI Messages) still queued.	com.cisco.ccbu:category = AWSSubsystem, component0 = CommandDispatcher	20

JMX Counter	Description	JMX Object Name	Threshold at Steady Phase
TasksQueued	The tasks (such as client requests and CTI messages) queued.	com.cisco.ccbu:category = AWSSubsystem, component0 = CommandDispatcher	20
RequestLongestTime	The maximum amount of time taken to complete an API request, in milliseconds.	com.cisco.ccbu:category = WebAppStats, component0 = AggregateWebappStats	4000
processCPULoad	The CPU load in this process.	java.lang:type = OperatingSystem	0.5
NumOfAgentsLoggedIn	The number of agents and supervisors logged in currently.	com.cisco.ccbu:category = AWSSubsystem, component0 = AWS Statistics Counter	2010

The following table lists the thresholds for counters related to Openfire processes.

Table 86: Counters Related to Openfire (JMX Port 12348)

JMX Counter	Description	JMX Object Name	Threshold at Login Phase
ExecutingTaskCount	The number of tasks (messages published to node) that are running currently.	com.cisco.ccbu.finesse.openfire: type = PubSubOrderedExecutorStatistics	60
QueuedTaskCount	The number of tasks in the queue. Messages that are getting published to a node are placed in the queue.	com.cisco.ccbu.finesse.openfire: type = PubSubOrderedExecutorStatistics	10
PeakThreadCount	The maximum number of threads run at the same time since the JVM was started or the peak was reset.	java.lang:type = Threading	300
ThreadCount	The number of threads running at the current moment.	java.lang:type = Threading	300
processCPULoad	The recent CPU usage for the Java Virtual Machine process.	java.lang:type = OperatingSystem	0.6

Check Logs

AppDynamics-related logs are used by the administrators for troubleshooting the failures that are encountered while enabling or disabling or testing the connectivity for performance monitoring from the Cloud Connect server.

AppDynamics related logs are used while debugging failures such as performance metrics not appearing in the AppDynamics controller. All AppDynamics-related logs are stored in their respective target nodes.

Audit Logs

The Audit trail for AppDynamics administrative operation that is initiated from the AppDynamics CLI on Cloud Connect server captures the user, action, and date/time details of the CLI operation.

command: `file get activelog orchestration-audit/audit.log*`

CLI Logs

Run the following command on the Cloud Connect node to retrieve AppDynamics CLI logs:

command: `file get activelog platform/log/cli*.log`

Ansible Logs

Run the following commands on the Cloud Connect node to retrieve AppDynamics related Ansible logs:

- Current transaction logs: `file get activelog ansible/ansible.log`
- Historical logs: `file get activelog ansible/ansible_history.log`

AppDynamics Logs (on the target host)

Refer to the following table for information on retrieving the AppDynamics-related Logs on target host:

Node	Performance Configuration	AppD Configuration
VOS	NA	file get activelog appdynamics/appdynamics.log file get activelog appdynamics/machineagent/logs file get activelog appdynamics/appserveragent/logs
ICM	<Install Directory> :\Cisco\AppDynamics \log\AppDynamics_ Perf_Configuration.log	<Install Directory> :\Cisco\AppDynamics \log\AppDynamics_ _Configuration.log
CVP	NA	<Install Directory> :\Cisco\CVP\ AppDynamics\log AppDynamics_ Configuration.log



Note For ICM and CVP, the install directory location changes based on your system configuration.

You can also view the below-mentioned logs using the Real-Time Monitoring Tool (RTMT):

- Ansible logs by selecting 'Ansible Controller' as the Cloud Connect service
- Audit logs by selecting 'Orchestration Audit' as the Cloud Connect service

- AppDynamics related logs by selecting 'Cisco APM Service' as the service on the target nodes

To download RTMT from Cloud Connect or target VOS nodes, use <https://FQDN:8443/plugins/CcmServRtmtPlugin.exe>.

For more information, refer to the Cisco Unified Real-Time Monitoring Tool Administration Guide at: <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>.

Things to Know

- AppDynamics cannot be enabled on FIPS-enabled deployment. Disable the FIPS mode before enabling AppDynamics.
- You can disable or enable AppDynamics through AppDynamics CLI on Cloud Connect. If AppDynamics is disabled and re-enabled with a different application name (taken from the inventory), a new instance is created in the AppDynamics controller with the new application name. However, the instance with the old application name exists and should be manually deleted by logging into the AppDynamics controller. The new application name will be updated in the configuration on the target node once AppDynamics is re-enabled successfully with the new application name.
- Performance monitoring for ECE, CCP and Cloud Connect is currently not supported.



APPENDIX **A**

MIB Results Example Appendix

- [Cisco Contact Center Applications MIB Results Example, on page 327](#)

Cisco Contact Center Applications MIB Results Example

The following example displays the data provided by the Cisco Contact Center Applications MIB SNMP agent on the target Unified ICM/Unified CCE installation icm70 in response to a series of SNMP GETNEXT requests beginning at node ciscoCcaMIB, OID 1.3.6.1.4.1.9.9.473.

For the purpose of example, assume that a single instance `cccaInstanceName.2 = acme` is installed with instance number “0” and that the following components are installed:

```
Router:
  cccaComponentName.instanceNumber(0).componentIndex(1) = RouterA
Logger:
  cccaComponentName.instanceNumber(0).componentIndex(2) = LoggerA
Peripheral Gateway:
  cccaComponentName.instanceNumber(0).componentIndex(3) = PG1A
Distributor Admin Workstation:
  cccaComponentName.instanceNumber(0).componentIndex(4) = Distributor
A single CRSP NIC has been installed as part RouterA:
  cccaNicType.instanceNumber(0).componentIndex(1).nicIndex(1) = crsp
A single Express PIM (acmiCRS) has been installed as part of PG1A:
  cccaPimPeripheralName.instanceNumber(0).componentIndex(3).cccaPimNumber(1) = ACD 1

cccaName.0 = cc-rgr1a
cccaDescription.0 = Cisco Intelligent Contact Management / IP
cccaVersion.0 = 7.1(1)
cccaTimeZoneName.0 = Eastern Standard Time
cccaTimeZoneOffsetHours.0 = 5
cccaTimeZoneOffsetMinutes.0 = 0
cccaSupportToolsURL.0 =
cccaInstanceName.0 = acme
cccaComponentType.0.1 = router(1)
cccaComponentType.0.2 = logger(2)
cccaComponentType.0.3 = pg(4)
cccaComponentType.0.4 = distAW(3)
cccaComponentName.0.1 = RouterA
cccaComponentName.0.2 = LoggerA
cccaComponentName.0.3 = PG1A
cccaComponentName.0.4 = Distributor
cccaComponentStatus.0.1 = started(4)
cccaComponentStatus.0.2 = started(4)
cccaComponentStatus.0.3 = started(4)
cccaComponentStatus.0.4 = started(4)
```

```

cccaComponentElmtName.0.1.1 = ccagent
cccaComponentElmtName.0.1.2 = crspnic
cccaComponentElmtName.0.1.3 = dbagent
cccaComponentElmtName.0.1.4 = mdsproc
cccaComponentElmtName.0.1.5 = router
cccaComponentElmtName.0.1.6 = rtsvr
cccaComponentElmtName.0.1.7 = testsync
cccaComponentElmtName.0.2.8 = configlogger
cccaComponentElmtName.0.2.9 = csfs
cccaComponentElmtName.0.2.10 = histlogger
cccaComponentElmtName.0.2.11 = recovery
cccaComponentElmtName.0.3.12 = mdsproc
cccaComponentElmtName.0.3.13 = opc
cccaComponentElmtName.0.3.14 = pgagent
cccaComponentElmtName.0.3.15 = acmipim
cccaComponentElmtName.0.3.16 = testsync
cccaComponentElmtName.0.4.17 = configlogger
cccaComponentElmtName.0.4.18 = rtclient
cccaComponentElmtName.0.4.19 = rtdist
cccaComponentElmtName.0.4.20 = updateaw
cccaComponentElmtRunID.0.1.1 = 3336
cccaComponentElmtRunID.0.1.2 = 2992
cccaComponentElmtRunID.0.1.3 = 3600
cccaComponentElmtRunID.0.1.4 = 3920
cccaComponentElmtRunID.0.1.5 = 4040
cccaComponentElmtRunID.0.1.6 = 3532
cccaComponentElmtRunID.0.1.7 = 4100
cccaComponentElmtRunID.0.2.8 = 948
cccaComponentElmtRunID.0.2.9 = 3248
cccaComponentElmtRunID.0.2.10 = 1248
cccaComponentElmtRunID.0.2.11 = 3272
cccaComponentElmtRunID.0.3.12 = 4724
cccaComponentElmtRunID.0.3.13 = 4864
cccaComponentElmtRunID.0.3.14 = 4964
cccaComponentElmtRunID.0.3.15 = 5236
cccaComponentElmtRunID.0.3.16 = 5228
cccaComponentElmtRunID.0.4.17 = 5460
cccaComponentElmtRunID.0.4.18 = 5488
cccaComponentElmtRunID.0.4.19 = 5504
cccaComponentElmtRunID.0.4.20 = 5536
cccaComponentElmtStatus.0.1.1 = active (5)
cccaComponentElmtStatus.0.1.2 = started (4)
cccaComponentElmtStatus.0.1.3 = active (5)
cccaComponentElmtStatus.0.1.4 = active (5)
cccaComponentElmtStatus.0.1.5 = active (5)
cccaComponentElmtStatus.0.1.6 = active (5)
cccaComponentElmtStatus.0.1.7 = active (5)
cccaComponentElmtStatus.0.2.8 = active (5)
cccaComponentElmtStatus.0.2.9 = active (5)
cccaComponentElmtStatus.0.2.10 = active (5)
cccaComponentElmtStatus.0.2.11 = active (5)
cccaComponentElmtStatus.0.3.12 = active (5)
cccaComponentElmtStatus.0.3.13 = active (5)
cccaComponentElmtStatus.0.3.14 = active (5)
cccaComponentElmtStatus.0.3.15 = standby (6)
cccaComponentElmtStatus.0.3.16 = active (5)
cccaComponentElmtStatus.0.4.17 = active (5)
cccaComponentElmtStatus.0.4.18 = active (5)
cccaComponentElmtStatus.0.4.19 = active (5)
cccaComponentElmtStatus.0.4.20 = active (5)
cccaRouterSide.0.1 = sideA (1)
cccaRouterCallsPerSec.0.1 = 0
cccaRouterAgentsLoggedOn.0.1 = 0
cccaRouterCallsInProgress.0.1 = 0

```

```
cccaRouterDuplexPairName.0.1 = cc-rgrla
cccaRouterNicCount.0.1 = 1
cccaNicType.0.1.1 = crsp(5)
cccaNicStatus.0.1.1 = started(4)
cccaLoggerSide.0.2 = sideA(1)
cccaLoggerType.0.2 = standard(1)
cccaLoggerRouterSideAName.0.2 = cc-rgrla
cccaLoggerRouterSideBName.0.2 = cc-rgrla
cccaLoggerDuplexPairName.0.2 = cc-rgrla
cccaLoggerHDSReplication.0.2 = 0
cccaDistAwSide.0.4 = sideA(1)
cccaDistAwType.0.4 = standard(0)
cccaDistAwAdminSiteName.0.4 = cc-rgrla
cccaDistAwRouterSideAName.0.4 = cc-rgrla
cccaDistAwRouterSideBName.0.4 = cc-rgrla
cccaDistAwLoggerSideAName.0.4 = cc-rgrla
cccaDistAwLoggerSideBName.0.4 = cc-rgrla
cccaDistAwDuplexPairName.0.4 = cc-rgrla
cccaDistAwHDSEnabled.0.4 = 0
cccaDistAwWebViewEnabled.0.4 = false(2)
cccaDistAwWebViewServerName.0.4 =
cccaPgNumber.0.3 = 1
cccaPgSide.0.3 = sideA(1)
cccaPgRouterSideAName.0.3 = cc-rgrla
cccaPgRouterSideBName.0.3 = cc-rgrla
cccaPgDuplexPairName.0.3 = cc-rgrla
cccaPgPimCount.0.3 = 1
cccaPimPeripheralName.0.3.1 = ACD 1
cccaPimPeripheralType.0.3.1 = acmiCRS(19)
cccaPimStatus.0.3.1 = started(4)
cccaPimPeripheralHostName.0.3.1 = LabHost
```




APPENDIX B

Unified ICM/Unified CCE SNMP Notifications

SNMP Notifications



- Note**
1. The message ID also contains the severity in the two most significant bits of the integer value. The message ID value shown is with these two bits masked to zero.
 2. Alarms with an asterisk (*) next to the Message ID are deemed to be critical alarms.
 3. The $\%n$ variable (where n is a numeric value) indicates a substitution field whereby node-specific or process-specific information is inserted.

- [Administrative Data Server SNMP Notifications, on page 332](#)
- [Node Manager SNMP Notifications, on page 332](#)
- [Message Delivery Service SNMP Notifications, on page 340](#)
- [Router SNMP Notifications, on page 343](#)
- [Logger SNMP Notifications, on page 353](#)
- [Peripheral Gateway SNMP Notifications, on page 361](#)
- [CTI SNMP Notifications, on page 367](#)
- [Live Data Events, on page 376](#)
- [Live Data TIP Server SNMP Notifications, on page 393](#)
- [Outbound Option SNMP Notifications, on page 398](#)
- [ICM Network Interface Controller SNMP Notifications, on page 410](#)
- [TDM Peripheral Gateway SNMP Notifications, on page 449](#)

Administrative Data Server SNMP Notifications

Table 87: Administrative Data Server Events

Message ID (hex)	Property	Value
106003A	Message	World Wide Web Publishing Service may be down. ICM is unable to communicate with web server.
	Severity	Error
	Type	Raise
	Description	World Wide Web Publishing Service may be down. ICM is unable to communicate with web server.
	Action	If the World Wide Web Publishing Service is not running, restart it or look for the messages in the IIS error log.
106003B	Message	World Wide Web Publishing Service is up.
	Severity	Informational
	Type	Clear
	Description	World Wide Web Publishing Service is up.
	Action	No action is required.

Node Manager SNMP Notifications

Table 88: Node Manager SNMP Notifications

Message ID (hex)	Property	Value
1028101	Message	%1 Node Manager initializing.
	Severity	Warning
	Type	Clear
	Description	The node management library, common to all ICM processes, is initializing itself. This is a standard practice when a process (re)starts.
	Action	No action is required.

Message ID (hex)	Property	Value
1028103	Message	The operator requested for the shutdown, %1 Node Manager is now functional.
	Severity	Informational
	Type	Clear
	Description	The Node Manager successfully started. The Node Manager shutdown because the operator requested a clean shutdown of the ICM node.
	Action	No action is required.
1028104	Message	%1 Node Manager started. Last shutdown was due to system shutdown.
	Severity	Informational
	Type	Clear
	Description	The Node Manager successfully started. The last reason the Node Manager stopped was because a clean shutdown of the node was requested by the operator.
	Action	No action is required.
1028105	Message	The operator/administrator has shutdown the ICM software on: %1.
	Severity	Warning
	Type	Raise
	Description	The Node Manager on the ICM node has given the command to stop ICM services. This happens when an operator/administrator stop the ICM services using ICM Service Control, "nmstop", "net stop", Control Panel Services, or shutdown the node.
	Action	Contact the operator/administrator to determine the reason for the shutdown.
1029101	Message	%1 Node Manager Manager started.
	Severity	Informational
	Type	Clear
	Description	The Node Manager process (which supervises the Node Manager) has started.
	Action	No action is required.

Message ID (hex)	Property	Value
102C101	Message	Node: %1, critical process: %2, has terminated. Rebooting node.
	Severity	Error
	Type	Raise
	Description	A critical process required to run the ICM software on this node has terminated execution. The Node Manager is forced to reboot the node.
	Action	Contact the technical assistance center.
102C103	Message	Node: %1, restarting process: %2.
	Severity	Warning
	Type	Clear
	Description	The Node Manager is restarting a process.
	Action	No action is required.
102C107	Message	The last shutdown was to reboot the Node Manager after the failure of critical process. %1 Node Manager started.
	Severity	Informational
	Type	Clear
	Description	The Node Manager requested the shutdown since a critical process for the node failed. The Node Manager started.
	Action	No action is required.
102C108	Message	The reason for the last shutdown is unknown. Possible causes includes a power failure, a system failure or a Node Manager exit. %1 Node Manager started.
	Severity	Error
	Type	Clear
	Description	The Node Manager unable to determine the reason for the system restart. Possible causes are power failure, a system failure (e.g. a Windows blue screen), a system not responding (in which an operator is forced to reboot), or a Node Manager exit. The Node Manager started.
	Action	Contact the technical assistance center.

Message ID (hex)	Property	Value
102C109	Message	Node: %4, process: %5, exited after %1 seconds. Minimum required uptime for process: %5 is %2 seconds. Delaying process restart for %3 seconds.
	Severity	Warning
	Type	Raise
	Description	A process exited after running for '%1' seconds. Such processes must run for a minimum amount of time before the Node Manager will automatically restart them after they terminate. The Node Manager will restart the process after delaying a number of seconds for other environmental changes to complete.
	Action	No action is required.
102C10A	Message	Node: %2, restarting process: %3, after having delayed restart for %1 seconds.
	Severity	Warning
	Type	Clear
	Description	The Node Manager is restarting a process after the requisite delay.
	Action	No action is required.
102C10B	Message	Terminating process: %2.
	Severity	Error
	Type	Raise
	Description	The Node Manager reports the termination of a process.
	Action	No action is required.
102C10C	Message	Node: %1, process: %2, exited after having detected a software failure.
	Severity	Error
	Type	Raise
	Description	A process exited (terminated itself) after it detected an internal software error.
	Action	If the process continues to terminate itself, call the technical assistance center for help in diagnosing the problem.

Message ID (hex)	Property	Value
102C10D	Message	Node: %1, process: %2, has detected a failure. Node Manager is restarting the process.
	Severity	Warning
	Type	Raise
	Description	The specified process has detected a situation that requires it to ask the Node Manager to restart it. This often indicates a problem external to the process itself (for example, some other process may have failed).
	Action	Node Manager on the ICM node will restart the process. The node should be checked to ensure that it is online. The process logs may be examined for root cause.
102C10E	Message	Node: %1, process: %2, went down for an unknown reason. Exit code: %3. It will be automatically restarted.
	Severity	Error
	Type	Raise
	Description	The specified process exited (terminated) with the indicated exit code. This termination is unexpected; the process died for an unknown reason. It will be automatically restarted.
	Action	Determine if the process has returned to service or has stayed offline. If the process is offline or "bouncing", determine root cause from the process logs.
102C10F	Message	Node: %3, process: %4, is down after running for %1 seconds. It will restart after delaying %2 seconds for related operations to complete.
	Severity	Warning
	Type	Raise
	Description	Specified process is down after running for the indicated number of seconds. It will restart after delaying for the specified number of seconds for related operations to complete.
	Action	Determine if the process has returned to service or has stayed offline. If the process is offline or "bouncing", determine root cause from the process logs.

Message ID (hex)	Property	Value
102C110	Message	Node: %1, process: %2, successfully reinitialized after restart.
	Severity	Warning
	Type	Clear
	Description	A process was successfully restarted.
	Action	No action is required.
102C111	Message	Node: %1, process: %2, successfully started.
	Severity	Informational
	Type	Clear
	Description	The process was successfully started.
	Action	No action is required.
102C112	Message	Node: %1, process: %2, exited cleanly and requested that it be restarted by the Node Manager.
	Severity	Warning
	Type	Raise
	Description	A process terminated itself successfully, and has requested the Node Manager to restart it.
	Action	No action is required.
102C113	Message	Node: %1, process: %2, exited from Ctrl-C or window close.
	Severity	Warning
	Type	Raise
	Description	A process exited as a result of a CTRL-C request or a request to close the process's active window.
	Action	No action is required.

Message ID (hex)	Property	Value
102C114	Message	Node: %1, process: %2, exited and requested that the Node Manager reboot the system.
	Severity	Error
	Type	Raise
	Description	A process terminated itself successfully but, due to other conditions, has requested that the Node Manager to reboot the system.
	Action	No action is required.
102D101	Message	%3 Node Manager exited after having been up for %1 seconds. Scheduling system reboot in %2 seconds.
	Severity	Error
	Type	Raise
	Description	The Node Manager has itself exited after having run for "%1" seconds. The system will be rebooted after waiting a few seconds for related operations to complete.
	Action	Contact the technical assistance center.
102D102	Message	%2 Node Manager exited after having been up for %1 seconds. Auto-reboot is disabled. Will attempt service restart.
	Severity	Error
	Type	Raise
	Description	The Node Manager has itself exited after having run for "%1" seconds. The system cannot be rebooted since auto-reboot is disabled. The Node Manager will attempt to restart the service.
	Action	Contact the technical assistance center.
102D103	Message	%3 Node Manager requested reboot after having been up for %1 seconds. Scheduling system reboot in %2 seconds.
	Severity	Error
	Type	Raise
	Description	The Node Manager has requested the system to be rebooted after having run for "%1" seconds. The system will be rebooted after waiting a few seconds for related operations to complete.
	Action	Contact the technical assistance center.

Message ID (hex)	Property	Value
102D104	Message	%2 Node Manager requested reboot after having been up for %1 seconds. Auto-reboot is disabled. Will attempt service restart.
	Severity	Error
	Type	Raise
	Description	The Node Manager has requested the system to be rebooted after having run for "%1" seconds. The system cannot be rebooted since auto-reboot is disabled. The Node Manager Manager will attempt to restart the service.
	Action	Contact the technical assistance center.
102D105	Message	%2: A critical process has requested a reboot after the service has been up for %1 seconds. Auto-reboot on process request is disabled. Will attempt service restart.
	Severity	Error
	Type	Raise
	Description	A critical process has requested a reboot after the service has been up for "%1" seconds. The system cannot be rebooted since auto-reboot on process request is disabled. The Node Manager Manager will attempt to restart the service.
	Action	Contact the technical assistance center.
102D106	Message	%3: A critical process has requested a reboot after having been up for %1 seconds. Scheduling system reboot in %2 seconds.
	Severity	Error
	Type	Raise
	Description	A critical process has requested the system to be rebooted after having run for "%1" seconds. The system will be rebooted after waiting "%2" seconds.
	Action	Contact the technical assistance center.

Message Delivery Service SNMP Notifications

Table 89: Message Delivery Service SNMP Notifications

Message ID (hex)	Property	Value
10F8004	Message	Device: %1, path changing to idle state.
	Severity	Informational
	Type	Clear
	Description	The indicated device is using this side of the central controller for its idle communication path (and is therefore using the other side of the central controller for its active communication path).
	Action	No action is required.
10F8005	Message	Device: %1, path changing to active state.
	Severity	Informational
	Type	Clear
	Description	The indicated device is using this side of the central controller for its active communication path.
	Action	No action is required.
10F8007	Message	Device: %1, path realignment failed.
	Severity	Error
	Type	Raise
	Description	The indicated device failed to realign its message stream to this side of the central controller.
	Action	No action is required.
10F8008	Message	Device: %1, disconnected.
	Severity	Error
	Type	Raise
	Description	The indicated device has been disconnected from this side of the central controller. This may be caused by a network problem or device failure.
	Action	Remedy network problems, if any. Call the Cisco Systems, Inc. technical assistance center in the event of a software failure on the device.

Message ID (hex)	Property	Value
10F800E	Message	Device: %1, path reset.
	Severity	Warning
	Type	Raise
	Description	The communication path between this side of the central controller and the indicated device has been reset to an initial state.
	Action	No action is required.
10F800F	Message	Device: %1, initializing message stream.
	Severity	Informational
	Type	Clear
	Description	The indicated device is initializing its message stream with this side of the central controller.
	Action	No action is required.
10F801D	Message	The network communications between ICM router and Peripheral Gateway or NIC: %2 has been down for: %1 minutes.
	Severity	Warning
	Type	Raise
	Description	No communication path from the indicated device to this side of the central controller has existed for the indicated time period. This indicates either an extended network outage or an extended outage at the device.
	Action	One or more network links between the named device and the named side of the ICM router has failed. If alarms exist for BOTH routers, the site is offline. If alarms exist for one side of the router, then the site should be up but network redundancy is degraded. Communication (network) between the central controller (router) and the PG should be checked using "ping" and "tracert". Must have visible and visible high priority connection from PG to router. CCAG process on router and PGAG process on PG should be checked.

Message ID (hex)	Property	Value
1040010	Message	Synchronizer timed out trying to establish connection to peer.
	Severity	Warning
	Type	Raise
	Description	The MDS message synchronizer was unable to connect to its duplexed partner within the timeout period. Either the duplexed partner is down, or there is no connectivity to the duplexed partner on the private network.
	Action	Verify reliable network connectivity on the private network. Call the Cisco Systems, Inc. technical assistance center in the event of a software failure on the duplexed partner.
1040022	Message	Connectivity with duplexed partner has been lost due to a failure of the private network, or duplexed partner is out of service.
	Severity	Error
	Type	Raise
	Description	The MDS message synchronizer has lost connectivity to its duplexed partner. This indicates either a failure of the private network, or a failure of the duplexed partner.
	Action	Confirm services are running on peer machine. Check MDS process to determine if it is paired or isolated. Ping test between peers over the private network. Check PGAG and MDS for TOS (Test Other Side) messages indicating the private network has failed and MDS is testing the health of the peer over the public network.
1040023	Message	Communication with peer Synchronizer established.
	Severity	Informational
	Type	Clear
	Description	The MDS message synchronizer has established communication with its duplexed partner.
	Action	No action is required.

Message ID (hex)	Property	Value
104802A	Message	MDS time delivery queue size is increasing, current size is: %1, but will continue to send messages.
	Severity	Warning
	Type	Single-State Raise
	Description	MDS time delivery queue size is increasing over time.
	Action	Ensure that the ICM/IPCC configuration (# agents, # skills/agent, # PGs) is within the supported limit.

Router SNMP Notifications

Table 90: Router SNMP Notifications

Message ID (hex)	Property	Value
12B0013	Message	Application Gateway has failed. Application Gateway ID: %1.
	Severity	Error
	Type	Raise
	Description	An application gateway connection has failed. This means that the application gateway process has attempted to connect to the host the number of times indicated in the Session Retry Limit field and has failed. It will not try to reconnect again until the connection is taken out of service and brought back into service.
	Action	Determine why the Application Gateway cannot connect to the host. Verify the connection between the two VMs. After fixing the issue, take the Application Gateway out of service and then bring it back in service.
12B001F	Message	Application Gateway has connected with the host. Application Gateway ID: %1.
	Severity	Informational
	Type	Clear
	Description	The application gateway is now connected to the host process.
	Action	No action is required.

Message ID (hex)	Property	Value
12B0020	Message	Application Gateway is not connected to the host. Application Gateway ID: %1; routing may be impacted.
	Severity	Error
	Type	Raise
	Description	An external application used in some scripts has disconnected from the specified Application Gateway. Error recovery mechanisms will attempt to reconnect. Routing may be impacted.
	Action	Verify the connection properties in the Application Gateway configuration. If the host application was off-line for a long time, restart the Application Gateway to reconnect.
12B0030	Message	Contact share node connection to Live Data %1 is Up.
	Severity	Informational
	Type	Clear
	Description	The Contact Share node connection to Live Data is up.
	Action	No action is required.
12B0031	Message	Contact share node connection to Live Data %1 is Down.
	Severity	Error
	Type	Raise
	Description	The Contact Share node connection to Live Data is down.
	Action	Check that Live Data is running. You can verify and update the Live Data configuration with the csmachineinventory command-line tool on the AW VMs.
12B0034	Message	Contact share node has determined that none of the configured AW hosts are active or have current data.
	Severity	Error
	Type	Raise
	Description	The Contact Share node has determined that none of the configured AW hosts are active or have current data.
	Action	Make sure at least one AW is up and active. Tomcat service on AW should be up and running.

Message ID (hex)	Property	Value
12B0035	Message	Contact share node is able to connect to AW and is able to retrieve data.
	Severity	Informational
	Type	Clear
	Description	The Contact Share node is able to connect to the AW and is able to retrieve data.
	Action	None.
105007D	Message	Peripheral: %2 (ID: %1) is on-line.
	Severity	Informational
	Type	Clear
	Description	The specified peripheral is on-line to the ICM. Call and agent state information is being received by the Router for this site.
	Action	No action is required.
105007E	Message	ACD/IVR: %2 (ID: %1) is off-line and not visible to the Peripheral Gateway. Routing to this site is impacted.
	Severity	Error
	Type	Raise
	Description	The specified ACD/IVR is not visible to the Peripheral Gateway. No call or agent state information is being received by the Router from this site. Routing to this site is impacted.
	Action	If Peripheral Gateway is also offline per messaging (message ID 10500D1) or "rttest" result, then first proceed with troubleshooting for Peripheral Gateway off-line alarm. Otherwise ACD/IVR Vendor should be contacted for resolution.
10500D0	Message	Physical controller: %2 (ID: %1) is on-line.
	Severity	Informational
	Type	Clear
	Description	The Router is reporting that physical controller "%2" is on-line.
	Action	No action is required.

Message ID (hex)	Property	Value
10500D1	Message	Peripheral Gateway: %2 (ID: %1) is not connected to the central controller or is out of service. Routing to this site is impacted.
	Severity	Error
	Type	Raise
	Description	The specified Peripheral Gateway is not connected to the central controller. It could be down. Possibly it has been taken out of service. Routing to this site is impacted.
	Action	Communication (network) between the central controller (Router) and the PG should be checked using "ping" and "tracert". You must have a visible high priority connection from the PG to the Router. The CCAgent process on the Router and the PGAgent process on the PG should be checked. The PG may have been taken out of service for maintenance.
10500D2	Message	PG has reported that peripheral: %2 (ID: %1) is operational.
	Severity	Informational
	Type	Clear
	Description	PG has reported that peripheral "%2" (ID "%1") is operational.
	Action	No action is required.
10500D3	Message	PG has reported that peripheral: %2 (ID: %1) is not operational.
	Severity	Error
	Type	Raise
	Description	This may indicate that the peripheral is off-line for maintenance or that the physical interface between the peripheral and the PG is not functioning.
	Action	Check that the peripheral is not off-line and that the connection from the peripheral to the PG is intact.

Message ID (hex)	Property	Value
10500F6	Message	Script table: %2 (ID: %1) is available only on side A.
	Severity	Informational
	Type	Raise
	Description	Script table "%2" is only available on the side A Router. If the side A Router goes down, no DBLookup requests can be processed as side B cannot access the script table.
	Action	Configure a script table on side B that is identical to that on side A.
10500F7	Message	Script table: %2 (ID: %1) is available only on side B.
	Severity	Informational
	Type	Raise
	Description	Script table "%2" is only available on the side B Router. If the side B Router goes down, no DBLookup requests can be processed as side A cannot access the script table.
	Action	Configure a script table on side B that is identical to that on side A.
10500F8	Message	Script table: %2 (ID: %1) is not available on either side.
	Severity	Error
	Type	Raise
	Description	No DBLookup requests can be processed as script table "%2" is unavailable on either side of the central controller.
	Action	Configure a script table on either side A or side B, or both.
10500F9	Message	Script table: %2 (ID: %1) is available on both sides A & B.
	Severity	Informational
	Type	Clear
	Description	Script table "%2" is configured on both sides of the central controller.
	Action	No action is required.

Message ID (hex)	Property	Value
10500FF	Message	Side: %1: %2 process is OK.
	Severity	Informational
	Type	Clear
	Description	The Router is reporting that side "%1" process "%2" is OK.
	Action	No action is required.
1050100	Message	Process: %2 at the central site side: %1 is down.
	Severity	Error
	Type	Raise
	Description	This alarm only occurs for central controller (Router and Logger) processes. If the process for BOTH sides is down there is a total failure for that process. This could be part of Router shutdown. Critical processes: - "mds" (Router/Logger): coordinates messaging between duplexed Routers AND Loggers. When mds is down the central controller is down and no calls are being routed. - "rtr" (Router): call routing intelligence. - "clgr/hlgr" (Logger) - configuration/historical data processing to configuration database. - "rts" (Router): Real Time Server data feed from the Router to the Admin Workstations for reporting. - "rcv" (Logger Recovery): keeps the redundant historical databases synchronized between duplexed Loggers.
	Action	No action is required.
10501F1	Message	ICM node: %2 (ID: %1) is on-line.
	Severity	Informational
	Type	Clear
	Description	The specified node is on-line to the ICM.
	Action	No action is required.
10501F2	Message	ICM node: %2 (ID: %1) is off-line.
	Severity	Error
	Type	Raise
	Description	The specified node is not visible to the ICM. Distribution of real time data may be impacted.
	Action	No action is required.

Message ID (hex)	Property	Value
10501F6	Message	The Router's state size of: %1 MB is now below the alarm limit of: %2 MB.
	Severity	Informational
	Type	Clear
	Description	The Router's state size of "%1" MB is now below the alarm limit of "%2" MB.
	Action	No action is required.
10501F7	Message	The Router's state size of: %1 MB has grown beyond the alarm limit of: %2 MB.
	Severity	Error
	Type	Raise
	Description	The Router's state size of "%1" MB has grown beyond the alarm limit of "%2" MB. This may indicate a memory leak, or it may indicate that the customer's configuration size has grown larger. Large state sizes may cause problems when synchronizing Routers, so the bandwidth of the private link may also need to be investigated.
	Action	The alarm limit can be raised with the "rtsetting" tool.
10501F8	Message	ICM node: %2 (ID: %1), on system: %3, is on-line.
	Severity	Informational
	Type	Clear
	Description	The specified node is on-line to the ICM.
	Action	No action is required.
10501F9	Message	ICM node: %2 (ID: %1), on system: %3, is off-line.
	Severity	Error
	Type	Raise
	Description	The specified node is not visible to the ICM. Distribution of real time data may be impacted. This condition can exist briefly while the system is loading. If it does not clear, it may indicate a problem with the node or the communications paths that connect the Router and node.
	Action	Check the communication paths that connect the Router and the node.

Message ID (hex)	Property	Value
10501FD	Message	The Router has completed loading the initial configuration from the Logger.
	Severity	Informational
	Type	Clear
	Description	The specified node is on-line to the ICM.
	Action	No action is required.
10501FE	Message	The Router has not loaded a configuration from the Logger.
	Severity	Error
	Type	Raise
	Description	This condition indicates that the Router has not yet completed the initialization step of loading a configuration from the Logger. This condition can exist briefly while the system is loading. If it does not clear, it may indicate a problem with the Logger or the communications paths that connect the Router and the Logger.
	Action	Check the communication paths that connect the Router and the Logger.
105023C	Message	The Router has detected that it is no longer synchronized with its partner.
	Severity	Error
	Type	Single-State Raise
	Description	The Router has detected that it is no longer synchronized with its partner. One result of this is that the Router might be routing some calls incorrectly.
	Action	Stop the Router on both sides. After both sides are completely stopped, restart both Routers. Alternate Action: Restart the Router on one side. After doing this, the Routers might still route some calls incorrectly, but they will be in sync.

Message ID (hex)	Property	Value
105029A	Message	Congestion level changed from: %1, with rejection percentage: %2, to congestion level: %3, with rejection percentage: %4, on: %5.
	Severity	Error
	Type	Raise
	Description	There is a change in the congestion level of the Router which implies that there is a change in the call rejection percentage also. When congestion control is enabled, the system will reject or treat the calls according to the congestion level and rejection percentage determined. When congestion control is disabled, the system will not reject or treat the calls until the congestion enabled option is turned on in the congestion control settings gadget.
	Action	The system has exceeded the designed capacity. Re-evaluate the system design if the congestion occurs frequently. When congestion control is disabled and the system is congested, you can turn on the congestion enabled option in the congestion control settings gadget to reject or treat the congested calls.
105029B	Message	The system congestion control level has moved to the normal operating level for the deployment: %1.
	Severity	Warning
	Type	Clear
	Description	The Router is currently not congested.
	Action	None
105029D	Message	Total number of agent skill group pairs: %1, exceeds the defined system default limit: %2.
	Severity	Error
	Type	Single-State Raise
	Description	Total number of agent skill group pairs exceeds the defined system default limit.
	Action	Log out agents or remove skill groups associated to the agent such that the agent skill group pair count does not exceed the defined system default limit.

Message ID (hex)	Property	Value
10502B0	Message	Error: %1
	Severity	Error
	Type	Raise
	Description	The Contact Share connection to the application gateway is down.
	Action	Open the application gateway list tool from the configuration manager tool and check the application gateway configuration for correct connection address properties.
10502B9	Message	Informational: %1
	Severity	Informational
	Type	Clear
	Description	The Contact Share connection to the application gateway is up.
	Action	No action is required.
10502BA	Message	Informational: %1
	Severity	Informational
	Type	Clear
	Description	The Contact Share connection to the application gateway is active.
	Action	No action is required.
10502BB	Message	Informational: %1
	Severity	Informational
	Type	Raise
	Description	The Contact Share connection to the application gateway is inactive.
	Action	No action is required.
10502BE	Message	The deployment has reached the maximum agent capacity of: %1.
	Severity	Warning
	Type	Raise
	Description	The number of logged-in agents has reached the maximum capacity supported by this deployment type.
	Action	No action is required.

Message ID (hex)	Property	Value
10502BF	Message	The deployment is below the maximum agent capacity of: %1.
	Severity	Informational
	Type	Clear
	Description	The number of logged-in agents is now below the maximum capacity supported by this deployment type.
	Action	No action is required.

Logger SNMP Notifications

Table 91: Logger SNMP Notifications

Message ID (hex)	Property	Value
12A0001	Message	Message Delivery Service (MDS) feed from the router to the logger has failed.
	Severity	Error
	Type	Raise
	Description	Indicates that the MDS event feed connection from the ICM router to the CSFS process on the logger has failed.
	Action	No action is required.
12A0002	Message	MDS is in service.
	Severity	Informational
	Type	Clear
	Description	Indicates MDS event feed connection from ICM router to CSFS process has connected.
	Action	If not a planned startup of the system, determine if the event is due to process, network, or system failure.

Message ID (hex)	Property	Value
12A0003	Message	Heartbeat event for: %1.
	Severity	Informational
	Type	N/A
	Description	Periodic message sent to indicate that the ICM Message Delivery Service (MDS) is in service and the system on which event management system processes reside can send events to the configured listener system. This message is also passed to the SNMP agent to indicate that the event stream is active.
	Action	No action is required.
12A4001	Message	SDDSN registration has been completed with system: %1, process: %2, using unique ID: %3. The registered system can now send diagnostic data via the SDDSN server.
	Severity	Informational
	Type	Clear
	Description	A system (via a particular process), connected to the SDDSN server has successfully registered as a valid endpoint using a unique ID. The system can now start sending diagnostic event data using the SDDSN server.
	Action	No action is required.
12A4002	Message	SDDSN unregistration was never received from system: %1, process: %2, using unique ID: %3. The registered system abruptly disconnected from the SDDSN server.
	Severity	Error
	Type	Raise
	Description	A system (via a particular process), connected to the SDDSN server has failed to unregistered as a valid endpoint using a unique ID. This indicates that the system abruptly disconnected from the SDDSN server.
	Action	This could indicate that the SDDSN server has failed or the TCP/IP connection to the server was lost. If this is a fault tolerant SDDSN server, check to see if the secondary SDDSN server has successfully re-registered the system). This would be indicated by a CLEAR condition to this alarm while the side of SDDSN that is reporting would be the other SDDSN server. If the primary SDDSN server is still running, check to see if you can ping between the system and the primary SDDSN server. Other scenarios include a simplex SDDSN server failure or lost TCP/IP connection, or the system that was communicating with the SDDSN server has somehow failed.

Message ID (hex)	Property	Value
12A4003	Message	SDDSN unregistration has been received from system: %1, process: %2, using unique ID: %3. The registered system has indicated that it will stop sending diagnostic data via the SDDSN server.
	Severity	Informational
	Type	Clear
	Description	A system (via a particular process), connected to the SDDSN server has successfully unregistered as a valid endpoint using a unique ID. This indicates that the system gracefully disconnected from the SDDSN server.
	Action	No action is required.
12A400A	Message	The SDDSN server is missing, or has outdated, resource files and cannot decipher messages for product: %1, (%3). Message ID = %2
	Severity	Error
	Type	Single-State Raise
	Description	An event has been received that the SDDSN server cannot decipher using the resource files (message DLLs) because they are missing or out of date. The SDDSN server has forwarded the ciphered event, and then disconnected the system that generated that event. %1 is the product number (in decimal). %2 is the Message ID that was sent. A value of 0 indicates that none of the messages can be deciphered. %3 is the name of the product.
	Action	The SDDSN server needs to have an updated installation of the resource files that are shipped with the product (%3). If %3 indicates 'Unknown', contact the technical assistance center to get a correlation between %1 and the actual product name. Install the updated support files for that product on the SDDSN server and restart it. This update will contain files named MSGSn.DLL and CATn.DLL where the 'n' should be replaced with the number %1 from this error message (e.g. MSGS2.DLL, CAT2.DLL, etc.).
12A4010	Message	The client system: %3, attempted to send an incompatible version: %1, SDDSN event. The current version supported is: %2.
	Severity	Error
	Type	Single-State Raise
	Description	An event has been received by a client system using an incompatible version of the SDDSN protocol.
	Action	The client system needs to be configured to send the correct version of the SDDSN protocol, or the SDDSN server needs to be upgraded to support the desired version.

Message ID (hex)	Property	Value
118C002	Message	%1%% of the available free space is used in database :%2.
	Severity	Informational
	Type	Single-State Raise
	Description	%1%% of the available free space is used in %2 database. This is an indication of how full the database is. When this value gets too high, the Logger will begin deleting the oldest historical records from the database.
	Action	Change the purge interval to save data for a shorter period of time. If this is not practical, add more disk space to the system and add disk devices to the database by using SQL Server Management Studio.
118C00C	Message	%1%% of the available log space is used in database: %2.
	Severity	Informational
	Type	Single-State Raise
	Description	%1%% of the available log space is used in the %2 database.
	Action	No action is required.
118C00F	Message	Begin automatic purge: %1%% of the available data space is used in database: %2.
	Severity	Warning
	Type	Raise
	Description	The automatic purge is being run in order to keep the database from running out of space. The parameters for the daily purge need to be adjusted to match the database storage capacity.
	Action	Contact the technical assistance center.
118C010	Message	Automatic purge complete: %1%% of the available data space is used in database: %2.
	Severity	Warning
	Type	Clear
	Description	The automatic purge has been run in order to keep the database from running out of space. The parameters for the daily purge need to be adjusted to match the database storage capacity.
	Action	No action is required.

Message ID (hex)	Property	Value
118C015	Message	Connected to client: %1, on port: %2.
	Severity	Informational
	Type	Clear
	Description	The Logger successfully connected to a client system.
	Action	No action is required.
118C017	Message	Logger or HDS connection to client: %1, on port: %2, either went out of service or has been broken.
	Severity	Informational
	Type	Raise
	Description	Logger or HDS on the specified TCP/IP connection and port number either went out of service or communication has been broken.
	Action	The Historical Data Server (HDS) or the peer Logger (on the other side of the duplexed central controller) is no longer getting its historical feed from this Logger. This can occur due to networking outages, SQL issues on the Logger or HDS, or the Logger or the HDS may have been shut down or otherwise disabled.
118C033	Message	Cannot find routing client with network routing client: %1, on server: %2, in database: %3; unable to replicate data to customer: %4, on CICR instance: %5.
	Severity	Warning
	Type	Single-State Raise
	Description	CICR replication must find a routing client in the database with a matching network routing client. Otherwise, it cannot translate the routing client ID foreign key in the dialed number or label properly. CICR replication is unable to complete the replication in this case.
	Action	No action is required.

Message ID (hex)	Property	Value
118C034	Message	Cannot find customer: %1, or instance: %2, on server: %3, in database: %4. Unable to replicate to customer: %1, on CICR instance: %2.
	Severity	Warning
	Type	Single-State Raise
	Description	CICR replication must find a customer and instance in the database with matching names. Otherwise, it cannot translate the customer definition ID foreign key in the dialed number or label properly. CICR replication is unable to complete the replication in this case.
	Action	No action is required.
118C035	Message	Dialed number or label exists with duplicate key on server: %1, in database %2; unable to replicate to customer: %3. on CICR Instance %4
	Severity	Warning
	Type	Single-State Raise
	Description	CICR replication has found that inserting the dialed number or label would cause a duplicate key error. Therefore, the dialed number or label cannot be inserted. CICR replication is unable to complete the replication in this case.
	Action	No action is required.
118C036	Message	Duplicate key exists for dialed number with enterprise name: %1.
	Severity	Warning
	Type	Single-State Raise
	Description	CICR replication has found that a dialed number already exists with this enterprise name. Therefore, it cannot insert the new dialed number. CICR replication is unable to complete the replication in this case.
	Action	No action is required.

Message ID (hex)	Property	Value
118C037	Message	Duplicate key exists for dialed number with routing client ID: %1, and dialed number string: %2.
	Severity	Warning
	Type	Single-State Raise
	Description	CICR replication has found that a dialed number already exists with this routing client ID and dialed number string. Therefore, it cannot insert the new dialed number. CICR replication is unable to complete the replication in this case.
	Action	No action is required.
118C038	Message	Duplicate key exists for label with routing client ID: %1, and label string: %2.
	Severity	Warning
	Type	Single-State Raise
	Description	CICR replication has found that a label already exists with this routing client ID and label string. Therefore, it cannot insert the new label. CICR replication is unable to complete the replication in this case.
	Action	No action is required.
118C039	Message	CICR replication on side%1 is now active.
	Severity	Informational
	Type	Clear
	Description	The CICR replication process is active.
	Action	No action is required.
118C03A	Message	CICR replication on side%1 is now inactive.
	Severity	Informational
	Type	Raise
	Description	The CICR replication process is inactive.
	Action	No action is required.

Message ID (hex)	Property	Value
118C03D	Message	Invalid host name is configured for customer: %1. Use the Configure ICM tool to re-configure the host name for customer: %1.
	Severity	Error
	Type	Single-State Raise
	Description	Invalid host name has been configured for the customer.
	Action	Use the ConfigICR->ICR_NODE to change the host name or system name and re-start the CICR replication process.
118C03E	Message	CICR replication failed to update CICR instance: %1, due to commit update CC transaction failure. Unable to rReplicate to customer: %1. Check and correct the errors.
	Severity	Warning
	Type	Single-State Raise
	Description	CICR replication failed to update the configuration change due to the error caused by the "commit update CC transaction" failure.
	Action	No action is required.
118C040	Message	Found %1 records with date/time greater than current central controller time: %2 in table: %3. Check and correct the errors.
	Severity	Warning
	Type	Single-State Raise
	Description	Found historical records with date/time greater than current central controller time. Delete the records which have date time greater than the current central controller time.
	Action	No action is required.
118C048	Message	NICR replication on side%1 is now inactive.
	Severity	Informational
	Type	Raise
	Description	The NICR replication process is inactive.
	Action	No action is required.

Message ID (hex)	Property	Value
118C049	Message	NICR replication on side%1 is now active.
	Severity	Informational
	Type	Clear
	Description	The NICR replication process is active.
	Action	No action is required.
118C051	Message	Invalid host name: %1, is configured for primary distributor for customer: %2. Use the Configure ICM tool to re-configure the primary distributor for customer: %2.
	Severity	Error
	Type	Single-State Raise
	Description	Invalid primary distributor has been configured for the customer, or the system is unable to resolve the hostname for the named primary distributor for some reason.
	Action	Use the ConfigICR->ICR_NODE to change the host name or system name and re-start the CICR replication process. Alternatively, check name resolution for the specified host name.

Peripheral Gateway SNMP Notifications

Table 92: Peripheral Gateway SNMP Notifications

Message ID (hex)	Property	Value
108C020	Message	The Enterprise CTI Server associated with this Peripheral Gateway is on-line on: %1.
	Severity	Informational
	Type	Clear
	Description	The Enterprise CTI server associated with this Peripheral Gateway is on-line. Enterprise CTI Client applications are able to connect to the server and exchange call and agent data.
	Action	No action is required.

Message ID (hex)	Property	Value
108C021	Message	The Enterprise CTI server associated with this Peripheral Gateway is down.
	Severity	Error
	Type	Raise
	Description	The Enterprise CTI server associated with this Peripheral Gateway is off-line. Enterprise CTI client applications are not able to connect to the server and exchange call and agent data.
	Action	Review the CTI server events and logs.
108C02B	Message	OPC has detected that it is no longer synchronized with its partner.
	Severity	Error
	Type	Single-State Raise
	Description	OPC has detected that it is no longer synchronized with its partner.
	Action	No action is required.
1088085	Message	PG has failed activation request for %1 consecutive times.
	Severity	Error
	Type	Single-State Raise
	Description	PG has failed activation and will be restarted.
	Action	No action is required.
13E0002	Message	Message Integration Service was unable to connect to: %1%2, on: %3, TCP/IP port: %4.
	Severity	Error
	Type	Raise
	Description	Message Integration Service (MIS) was unable to connect to the indicated component and address.
	Action	Confirm component is available, configuration of IP address(es) and port(s) are correct, and network connectivity would allow for connection.

Message ID (hex)	Property	Value
13E0003	Message	Connection to: %1%2, address: %3:%4, succeeded.
	Severity	Informational
	Type	Clear
	Description	Message Integration Service (MIS) was able to connect to the indicated component and address.
	Action	No action is required.
13E0004	Message	Message Integration Service was unable to open a session to: %1%2.
	Severity	Error
	Type	Raise
	Description	Message Integration Service (MIS) was unable to open a session to the indicated component.
	Action	No action is required.
13E0005	Message	Session to: %1%2, opened.
	Severity	Informational
	Type	Clear
	Description	Message Integration Service (MIS) was able to open a session to the indicated component and address.
	Action	No action is required.
13E0006	Message	Trunk group: %1, trunk: %2; received in message from VRU-%3; not configured.
	Severity	Error
	Type	Single-State Raise
	Description	A message pertaining to the indicated trunk group and trunk has not been configured with MIS.
	Action	Configure extension, trunk group, and trunk in MIS.

Message ID (hex)	Property	Value
13E0007	Message	Call tracking error: %1.
	Severity	Error
	Type	Single-State Raise
	Description	A call within MIS could not be tracked successfully.
	Action	Determine where tracking problem occurred and correct (for MIS problem, it could be MIS, VRU, or PG).
1540002	Message	An error occurred on the TCP/IP connection between the ACMI ACD server (CTI) and the ACMI peripheral gateway. ACMI peripheral gateway is offline.
	Severity	Error
	Type	Raise
	Description	An error occurred on the connection between the ACMI ACD server (CTI) and the ACMI peripheral gateway. ACMI peripheral gateway is offline.
	Action	If ACMI peripheral gateway does not re-attach, contact the technical assistance center.
1540003	Message	Peripheral status was DOWN, going NORMAL. ACMI peripheral gateway is online.
	Severity	Informational
	Type	Clear
	Description	Peripheral status was DOWN, going NORMAL. ACMI peripheral gateway is online.
	Action	No action is required.
1540007	Message	The route register on the DN: %1, is operational.
	Severity	Informational
	Type	Clear
	Description	The DN is operational.
	Action	No action is required.

Message ID (hex)	Property	Value
1540008	Message	The route register failed for DN: %1.
	Severity	Error
	Type	Raise
	Description	The Permit Application Routing box on the child system is not checked for DN.
	Action	Check Permit Application Routing box.
1540009	Message	The route register failed for DN: %1.
	Severity	Error
	Type	Raise
	Description	You have configured a DN or DN for a translation route on the parent that doesn't exist on the child system. Don't forget to check 'Permit Application Routing' when adding it.
	Action	Add the DN on the child system and ensure that 'Permit Application Routing' is enabled.
154000A	Message	The route register failed for DN: %1.
	Severity	Error
	Type	Raise
	Description	You have configured a DN or DN for a translation route on the parent that doesn't exist on the child system. Don't forget to check 'Permit Application Routing' when adding it.
	Action	Add the DN on the child system and ensure that 'Permit Application Routing' is enabled.
154000B	Message	The route register failed for DN: %1.
	Severity	Error
	Type	Single-State Raise
	Description	You have specified an incorrect server peripheral ID in the PG Setup of the Gateway PG.
	Action	Correct the server peripheral ID in the PG Setup of the Gateway PG and restart the PG.

Message ID (hex)	Property	Value
154000C	Message	The route register failed for DN: %1.
	Severity	Error
	Type	Single-State Raise
	Description	Another Gateway PG has requested control of this DN. This is most likely due to an incorrect server hostname being configured.
	Action	Correct the server host name in the PG Setup of the Gateway PG and restart the PG.
154000D	Message	The peripheral ID: %1 given, is not valid.
	Severity	Error
	Type	Single-State Raise
	Description	You have specified an incorrect server peripheral ID in the PG Setup of the Gateway PG.
	Action	Correct the server peripheral ID in the PG Setup of the Gateway PG and restart the PG.
154000E	Message	Central controller connection on child down - ACMI peripheral gateway status DOWN.
	Severity	Error
	Type	Raise
	Description	Central controller connection on child down - ACMI peripheral gateway status DOWN.
	Action	No action is required.

CTI SNMP Notifications

Table 93: CTI SNMP Notifications

Message ID (hex)	Property	Value
12E8006	Message	CONNECTION MONITOR SERVICE: Enterprise CTI session established by client: %1 (%2) at: %3.
	Severity	Informational
	Type	Clear
	Description	An Enterprise CTI session has been opened by client ID %1 (signature %2) from IP address %3.
	Action	No action is required.
12E8007	Message	CONNECTION MONITOR SERVICE: Enterprise CTI session closed by client: %1 (%2) at: %3.
	Severity	Warning
	Type	Raise
	Description	The Enterprise CTI session with client ID %1 (signature %2) at IP address %3 has been closed by the client.
	Action	This indicates that an Enterprise CTI client application that is generally always connected to the Enterprise CTI Server has closed its connection. The CTI client application software may need to be checked for proper operation.
12E8008	Message	CONNECTION MONITOR SERVICE: Enterprise CTI session terminated with client: %1 (%2) at: %3.
	Severity	Error
	Type	Raise
	Description	The Enterprise CTI session with client ID %1 (signature %2) at IP address %3 has been terminated by the Enterprise CTI Server.
	Action	This indicates that an Enterprise CTI Client application that is generally always connected to the Enterprise CTI Server has been disconnected due to errors. If the problem persists, the CTI client application software may need to be checked for proper operation.

Message ID (hex)	Property	Value
12E800C	Message	Client: %1, object: %2, normal event report: %3.
	Severity	Informational
	Type	Clear
	Description	The Enterprise CTI client %1 application software has reported the following normal event for object %2: %3.
	Action	No action is required.
12E800D	Message	Client: %1, object: %2, warning event report: %3.
	Severity	Warning
	Type	Raise
	Description	The Enterprise CTI client %1 application software has reported the following warning for object %2: %3.
	Action	This indicates that the CTI client application software has detected a possible error or other abnormal condition and may need to be checked for proper operation.
12E800E	Message	Client: %1, object: %2, error event report: %3.
	Severity	Error
	Type	Raise
	Description	The Enterprise CTI client %1 application software has reported the following error for object %2: %3.
	Action	This indicates that the CTI client application software has detected an error condition and may need to be checked for proper operation.
12E800F	Message	A version 13 or prior CTI client ID: %1 (%2) at: %3, connected with agent multi line enabled.
	Severity	Warning
	Type	Raise
	Description	A CTI client: %1 (signature: %2) from IP address: %3 with a version prior to 14 has connected to CTI Server that supports multi-line phones. Problems may be encountered with that application depending upon what messages/devices, etc. it processes events for.
	Action	Check with the vendor of the software and see if they have ensured compatibility.

Message ID (hex)	Property	Value
12E8010	Message	A version 13 or prior CTI client ID: %1 (%2) at: %3, disconnected with agent multi line enabled.
	Severity	Warning
	Type	Clear
	Description	A CTI client %1 (signature %2) from IP address %3 with a version prior to 14 has connected to CTI Server that supports multi-line phones. Problems may be encountered with that application depending upon what messages/devices, etc. it processes events for.
	Action	Check with the vendor of the software and see if they have ensured compatibility.
12EC00E	Message	CTI Server was unable to forward ECC variables due to an overflow condition.
	Severity	Warning
	Type	Single-State Raise
	Description	CTI Server found too much data in ECC variables while processing messages. ECC Variables will not be forwarded for these messages.
	Action	This indicates that too many / too large ECC variables are configured in the system. Eliminate some ECC variables or reduce the size of existing ECC variables to alleviate this condition.
1560004	Message	CTI OS Server version: %2, is online. Connected to CTI Server at: %3. CTI Server protocol is: %1.
	Severity	Informational
	Type	Clear
	Description	Message indicating the version of CTI OS Server as well as the protocol version CTI OS Server uses to connect to CTI Server.
	Action	No action is required.

Message ID (hex)	Property	Value
1560005	Message	CTI OS Server version: %2, cycled because the connection to CTI Server at: %3, closed. CTI Server protocol is: %1.
	Severity	Warning
	Type	Raise
	Description	CTI OS Server has cycled itself because its connection to CTI Server closed. When CTI OS Server restarts, it will re-establish its connection to CTI Server.
	Action	This event usually occurs when the CTI Server process cycles. If this event is received and CTI Server was not manually cycled, please collect the CTI OS Server log as well as all PG logs and contact the technical assistance center.
1560006	Message	CTI OS Server version: %2, cycled because the connection to CTI Server at: %3, failed. CTI Server protocol is: %1.
	Severity	Error
	Type	Raise
	Description	CTI OS Server has cycled itself because its connection to CTI Server failed. When CTI OS Server restarts, it will re-establish its connection to CTI Server.
	Action	This event can occur when CTI OS is running on a heavily loaded system. If this event is received and CTI Server was not stopped, please check the total CPU usage as well as CTI OS Server CPU usage. If either total or CTI OS Server CPU usage is greater than 60%, please check the agent, team, and skill group configuration against published limits to ensure it is within tolerance.
1560007	Message	CTI OS Server has %1 messages in queue.
	Severity	Informational
	Type	Clear
	Description	The CTI OS Server incoming message is now below 10,000 messages.
	Action	No action is required.

Message ID (hex)	Property	Value
1560008	Message	CTI OS Server has %1 messages in queue.
	Severity	Warning
	Type	Raise
	Description	The CTI OS Server incoming message queue exceeded 10,000 messages. This might result in unwanted behavior.
	Action	This event can occur when CTI OS is running on a heavily loaded system. If this event is received, please check the total CPU usage as well as CTI OS Server CPU usage. If either total or CTI OS Server CPU usage is greater than 60%, please check the agent, team, and skill group configuration against published limits to ensure it is within tolerance.
1560009	Message	CTI OS Server has generated an exception in: %2, processing %3. Details: %4: %1 %5.
	Severity	Error
	Type	Single-State Raise
	Description	CTI OS Server generated an exception while processing a request or an event specified in this method.
	Action	This is an internal error in CTI OS Server's request and message processing logic. Please collect the CTI OS Server log as well as all PG logs and contact the technical assistance center.
156000A	Message	CTI OS Server has generated an exception in: %2, processing %3. Details: %4: %1 %5.
	Severity	Error
	Type	Single-State Raise
	Description	CTI OS Server generated an exception while processing the request or event specified in this method.
	Action	This is an internal error in CTI OS Server's request and message processing logic. Please collect the CTI OS Server log as well as all PG logs and contact the technical assistance center.

Message ID (hex)	Property	Value
156000B	Message	CTI OS Server's total amount of agent mode connections is: %1. This is within CTI OS Server's limit of: %2.
	Severity	Informational
	Type	Clear
	Description	CTI OS Server is current running with an acceptable number of agents connected to it.
	Action	No action is required.
156000C	Message	CTI OS Server's total amount of agent mode connections is: %1. This exceeds CTI OS Server's limit of: %2.
	Severity	Warning
	Type	Raise
	Description	CTI OS Server is currently running with an excessive number of agents connected to it.
	Action	Ensure that the number of agent's currently using the system is not more than the limit listed in the event's description. If there are custom CTI OS applications deployed in the contact center, make sure to understand how many connections those custom applications open to CTI OS Server. For example, if a custom application opens two connections to CTI OS Server, this will halve the number of agents that can connect to CTI OS Server.
156000D	Message	CTI OS Server's total amount of monitor mode connections is: %1. This is within CTI OS Server's limit of: %2.
	Severity	Informational
	Type	Clear
	Description	CTI OS Server is current running with an acceptable number of monitor-mode applications connected to it.
	Action	No action is required.

Message ID (hex)	Property	Value
156000E	Message	CTI OS Server's total amount of monitor mode connections is: %1. This exceeds CTI OS Server's limit of: %2.
	Severity	Warning
	Type	Raise
	Description	CTI OS Server is currently running with an excessive number of monitor-mode applications connected to it.
	Action	Ensure that the number of monitor mode applications connected to CTI OS Server does not exceed the limit listed in the event's description. If there are custom CTI OS applications deployed in the contact center, make sure to understand how many connections those custom applications open to CTI OS Server as well as what types of connections those applications open to CTI OS Server. For example, applications that appear to open an agent mode connection (presents a UI geared toward an agent) may also open a monitor mode connection in the background.
156000F	Message	CTI OS Server's monitor mode functionality has been re-enabled. Monitor mode functionality was previously disabled after %1 failed attempts to access monitor mode functionality.
	Severity	Informational
	Type	Clear
	Description	CTI OS Server has re-enabled monitor mode functionality.
	Action	No action is required.

Message ID (hex)	Property	Value
1560010	Message	CTI OS Server's monitor mode functionality has been disabled after %1 failed attempts to access monitor mode functionality.
	Severity	Warning
	Type	Raise
	Description	CTI OS Server has disabled access to monitor mode functionality because an excessive number of consecutive failed attempts to access monitor mode functionality have occurred. An attempt to access monitor mode functionality fails when the CTI OS monitor mode password is incorrectly specified.
	Action	This event occurs when CTI OS security is enabled and a monitor password has been set. If this event is triggered, one or more applications have consecutively failed to supply the correct monitor mode password. Check the CTI OS Server log for lines containing the following text: security warning: client at @lt;ip_address@gt; failed to establish a monitor mode connection. Check to make sure that the CTI OS client at the given IP address is actually running a monitor mode client. If not, it is possible that there was an attempt to hack into CTI OS monitor mode functionality. If there is a CTI OS client at the given IP address, the client may have the wrong monitor mode password. If no action is taken and no further attempts to access monitor mode functionality fail, monitor mode functionality will unlock after the configured amount of time (15 minutes by default).
1560011	Message	After the CTI OS Server version %2 re-established the connection to CTI Server at: %3, configuration change was detected. The CTI OS Server will restart. CTI Server protocol is: %1.
	Severity	Warning
	Type	Raise
	Description	Upon re-establishment of the CTI Server Link, CTI OS Server detected a configuration change. CTI OS Server will restart to insure proper configuration.
	Action	This event can occur when CTI OS has lost connection to the CTI Server and the configuration has changed during that period.

Message ID (hex)	Property	Value
1560012	Message	The CTI OS Server version %2 connection to CTI Server at: %3 has closed. The CTI OS Server will attempt to re-establish the connection. CTI Server protocol is: %1.
	Severity	Warning
	Type	Raise
	Description	CTI OS Server's connection to the CTI Server has closed. CTI OS Server will attempt to re-establish the connection to the CTI Server. If Unsuccessful, CTI OS Server will restart.
	Action	This event usually occurs when the CTI Server closes the connection. If this event is received and CTI Server was not able to reconnect to the CTI Server, the CTI OS Server may cycle. Please collect the CTI OS Server log as well as all PG logs and contact the technical assistance center.
1560013	Message	CTI OS Server is within the supported limit for: %1 %2. %3.
	Severity	Informational
	Type	Clear
	Description	CTI OS Server is within the supported operational limit for this configuration/action.
	Action	No action is required.
1560014	Message	CTI OS Server is within the supported limit for %1 %2 has been exceeded. %3.
	Severity	Warning
	Type	Raise
	Description	The CTI OS Server is within the supported operational limit has been exceeded
	Action	This event occurs when a CTI OS Server is within the supported operational limit has been exceeded for either a configuration or action. This violation may adversely affect CTI OS performance. Please check the published operational limits for this release of CTI OS Server.

Live Data Events

Table 94: Live Data Events

Message ID (decimal)	Property	Value
107	Message	[server_address=%s]: Connection Terminated to ActiveMQ
	Severity	Informational
	Type	Raise
	Description	Informs JMS publisher connection to ActiveMQ service is down. JMS publisher terminated/stopped.
	Action	Ordinarily, no action required. However, if connection to JMS (ActiveMQ service) is down for extended periods of time, then, verify if ActiveMQ service status and evaluate overall system health, i.e., verify services are up, disk partitions have free space, system is not CPU starved, not swapping, not I/O bound, etc.
108	Message	[server_address=%s]: Connection Established to ActiveMQ
	Severity	Informational
	Type	Clear
	Description	Informs JMS publisher connection to ActiveMQ service is up. JMS publisher started, or, if connection lost, connection established.
	Action	No action required. Note, however, that if JMS connection is bouncing often, then, this could be an indication of a system-wide issue, so evaluate overall system health, i.e., verify services are up, disk partitions have free space, system is not CPU starved, not swapping, not I/O bound, etc.
301	Message	[message_error=%s]: Error initializing JMX MBean
	Severity	Error
	Type	Raise
	Description	Failure during creation of JMX bean for TIP statistical reporting, which can be linked to JMX services failure to initialize, lack of system resources, or incorrect configuration of JMX host/port.
	Action	Verify overall system health, i.e., services are up, disk partitions have free space, system is not CPU starved, not swapping, not I/O bound, etc. Attempt system restart, if problem persists, contact tech. support.

Message ID (decimal)	Property	Value
303	Message	[jmx_bean_name=%s]: JMX MBean registration failed
	Severity	Error
	Type	Raise
	Description	Failure during establishment of JMX bean for event spout (PG, Router, etc) operations. This means no operations to/from spouts will be possible via JMX.
	Action	Attempt system restart, if problem persists, contact tech. support.
304	Message	[jmx_bean_name=%s]: JMX MBean registration succeeded
	Severity	Error
	Type	Clear
	Description	Success in establishing JMX bean for event spout (PG, Router, etc) operations.
	Action	No action required.
405	Message	[connection_usage=%s] [server_address=%s] [state=%s] [message_error=%s] : Connection error
	Severity	Warning
	Type	Raise
	Description	Error during attempt to communicate (or establish connection) to CCE server (PG, Router, etc). This can be caused by: <ul style="list-style-type: none"> • Destination host/port not accepting connections. • Too many messages (from server) pending processing by Live Data. • Write to closed (by far-end) connection.
	Action	As follows: <ul style="list-style-type: none"> • Verify CCE server host/port configuration is correct, and port is open on host fire-wall. • Verify CPU availability to Live Data. If problem persists contact tech. support. • No action required for attempt to write to closed (by far-end) connection.

Message ID (decimal)	Property	Value
407	Message	[server_address=%s][tip_missed_heartbeats=%d]: Heatbeat Missed on TIP connection
	Severity	Warning
	Type	Clear
	Description	Missed one heartbeat to CCE server is not uncommon, and it is typically linked to a busy system. Live Data uses heartbeat to track the health of a CCE connection, and if too many (configurable) heartbeats are lost it will close and (attempt) to re-open the connection.
	Action	No action required.
501	Message	[properties=%s]: TIP Controller Stopped
	Severity	Critical
	Type	Raise
	Description	Indicates spout communication controller, responsible for CCE message processing, has terminated/stopped. This can happen on following scenarios: <ul style="list-style-type: none"> • Failover to standby cluster node. • JMX reset connection request. • System shutdown.
	Action	On failover: determine failover root cause and correct it. Start with overall system health, i.e., services are up, disk partitions have free space, system is not CPU starved, not swapping, not I/O bound, etc. If no reason is found, or reason cannot be corrected, contact tech. support. For all the other reasons: no action required.
502	Message	[tip_client_seggrp=%s][tip_client_app_seqnum=%s][properties=%s]: TIP Controller Started
	Severity	Critical
	Type	Clear
	Description	Indicates spout communication controller, responsible for CCE message processing, has started.
	Action	No action required.

Message ID (decimal)	Property	Value
503	Message	[server_address=%s] [message_error=%s]: Error in TIP Controller Processes
	Severity	Error
	Type	Raise
	Description	Indicates protocol error due to: <ul style="list-style-type: none"> • Request/response timeout • Unrecognized message format • Failure in message decoding • Failure in message processing
	Action	Protocol request/response timeouts are not uncommon and are typically linked to communication failure due to far-end port disconnect (i.e., attempt to write to a closed socket). For all other failures, contact tech. support.
505	Message	[message_error=Connection-%s]: Invalid TIP Configuration for
	Severity	Error
	Type	Raise
	Description	Configuration to CCE server is incomplete, or invalid. Port is not numeric in range 1-65565, host name contains invalid characters, etc.
	Action	Verify Live Data configuration and restart system.
507	Message	[server_address=%s] [tip_client_seqgrp=%s] [tip_server_seqgrp=%s]: TIP Sequence Group Mismatch
	Severity	Error
	Type	Raise
	Description	Indicates data loss during last CCE connection switch-over. PG/Router unavailable simultaneous to a communication loss to PG/Router corresponding side (A or B).
	Action	No action required. The system will issue a new sequence group, and request a snapshot to re-synch its internal state with that of the failed component.

Message ID (decimal)	Property	Value
509	Message	[server_address=%s][tip_client_seqgrp=%s][tip_server_seqgrp=%s]: TIP Message Gap between client and server
	Severity	Error
	Type	Raise
	Description	Indicates data loss during last CCE communication. PG/Router crash simultaneous to a communication loss to PG/Router corresponding side (A or B).
	Action	No action required. The system will request a snapshot to re-synch its internal state with that of the failed component.
511	Message	[server_address=%s]: TIP Controller switching Active Side
	Severity	Warning
	Type	Raise
	Description	Indicates spout communication controller has detected an active connection (to CCE server) is down, and that the standby connection to configured PG/Router will become active (switch-over). The PG/Router communication was severed, or the CCE server is no longer running.
	Action	Verify CCE server (PG, Router, etc) health.
512	Message	[server_address=%s][tip_client_seqgrp=%s][tip_server_seqgrp=%s]: TIP Message Synchronization Successful with TIP Server
	Severity	Error
	Type	Clear
	Description	Indicates that during a switch-over (from active connection to standby) the sequence number received by standby is in ascending order, and that it can be released from CCE server side. PG/Router unavailable, but Live Data state is not affected by it.
	Action	No action required.
515	Message	[server_address=%s][operation_type=%s]: TIP Protocol Request Failure
	Severity	Warning
	Type	Raise
	Description	Request to CCE server has failed, or timed out.
	Action	No action required.

Message ID (decimal)	Property	Value
517	Message	[server_address=%s] [message_error=%s] [operation_type=%s] : TIP Protocol Errors
	Severity	Error
	Type	Raise
	Description	Protocol error during response processing (of a request to CCE server) due to response to an invalid, or inexistent, pending request id. This can be linked to an expired request, as well as, an inexistent request.
	Action	No action required.
521	Message	[server_address=%s] [message_error=%s] : TIP Heartbeat Failure
	Severity	Error
	Type	Raise
	Description	Reached allowed number of heartbeat losses to CCE server. This will disconnect all CCE servers (PG, Router, etc) associated with a given CCE side (A or B). A switch over to other CCE server side (A or B) will be automatically initiated.
	Action	Determine network integrity between Live Data and CCE servers on failed side (A or B). Determine if CCE server (PG, Router, etc) is up and running.
523	Message	[server_address=%s] [message_error=%s] : Error in TOS Client
	Severity	Error
	Type	Raise
	Description	Indicates TOS (related to Live Data Cluster node state) protocol error. Possible error causes are: <ul style="list-style-type: none"> • Failure to start TOS communication • Failure during write to TOS far-end server
	Action	Verify Live Data configuration, restart system.

Message ID (decimal)	Property	Value
601	Message	[server_address=%s][message_error=%s]: Warning in TOS Client"
	Severity	Warning
	Type	Raise
	Description	Unable to send message to assess Live Data Cluster state on far end. Triggered by failure to receive cluster node state via JMS (ActiveMQ/Netbridge in this case), which can be caused by cluster node crash, network failure, ActiveMQ crash, or Netbridge crash.
	Action	Verify network integrity between Live Data cluster nodes. Verify ActiveMQ service is up, and cluster nodes configured for fail-over.
603	Message	[server_address=%s][message_error=%s]: TOS REQUEST RESPONSE latency alert.
	Severity	Warning
	Type	Raise
	Description	Request/response round trip time to cluster nodes is greater than configured seconds. This can be linked to network latency, or sluggish response from cluster node far end.
	Action	Verify network integrity between Live Data clusters nodes. Verify overall system health on all Live Data cluster nodes.
607	Message	[server_address=%s][missed_heartbeats]: Heatbeat Missed on TOS connection
	Severity	Warning
	Type	Raise
	Description	Missed one heartbeat to CCE server is not uncommon, and it is typically linked to a busy system. Live Data uses heartbeat to track the health of a CCE connection, and if too many (configurable) heartbeats are lost it will close and (attempt) to re-open the connection.
	Action	Verify network integrity between CCE server and Live Data.

Message ID (decimal)	Property	Value
609	Message	[server_address=%s] [message_error=%s]: TOS Heartbeat Failure
	Severity	Error
	Type	Raise
	Description	Reached allowed number of heartbeat losses to CCE server (PG, Router, etc). This will cause a disconnection followed by reconnection to CCE servers (PG, Router, etc).
	Action	Verify network integrity from CCE server (PG, Router, etc) to Live Data. Verify CCE server (PG, Router, etc) is up and running.
703	Message	[operation_error_desc=%s]: Camel Service Error
	Severity	Error
	Type	Raise
	Description	Failed to open connection to JMS (ActiveMQ) or to publish to indicated topic. Configuration to JMS (ActiveMQ) is incorrect, or service is down.
	Action	Verify Live Data configuration. Assess overall system health, i.e., services are up, disk partitions have free space, system is not CPU starved, not swapping, not I/O bound, etc. Note that, in case of ActiveMQ service down, the Live Data cluster will fail-over to standby node.
801	Message	[server_id=%s]: Spout failed to load UCCE Configuration
	Severity	Error
	Type	Raise
	Description	Error during load of Live Data configuration from AWDB. Dataset name pointing to AWDB, incorrectly configured in CUIC. location.
	Action	Using CUIC interface assure data set name for CUIC is correctly configured with address to AWDB. Ensure AWDB system is up and running. If problem persists, contact tech. support.
802	Message	[server_id=%s]: Spout loaded UCCE Configuration
	Severity	Informational
	Type	Clear
	Description	Live Data configuration, from AWDB, loaded to local memory.
	Action	No action required.

Message ID (decimal)	Property	Value
805	Message	[message_error=%s]: JMS Command Spout failed to Initialize
	Severity	Error
	Type	Raise
	Description	JMS command spout failed to initialize. Scenario JMS (ActiveMQ) communication was not possible via Camel, and an exception was thrown.
	Action	Verify Live Data configuration, and restart system. If problem persists, contact tech. support.
807	Message	[message_error=%s]: JMS Command Spout failed to Close
	Severity	Error
	Type	Raise
	Description	JMS command spout failed to close JMS connection.
	Action	No action required.
809	Message	[server_id=%s][tip_client_app_seqnum=%d][tip_server_app_seqnum=%d]: Invalid Application Sequence Number Received
	Severity	Error
	Type	Raise
	Description	During communication with CCE server, message sequence number was not in increasing order, and/or presented a gap. Possible data loss.
	Action	Gather logs and contact tech. support.
813	Message	[server_id=%s][message_error=%s]: Spout runtime error
	Severity	Error
	Type	Raise
	Description	Indicates event spout runtime error: <ul style="list-style-type: none"> • Zookeeper connection object could not instantiate or connect. • Establishment of JMS command queue listener failed. • JMX configuration could not be written to Zookeeper.
	Action	Verify Zookeeper service is up and running, and restart system. If problem persists, contact tech. support.

Message ID (decimal)	Property	Value
815	Message	[server_id=%s]: Spout lost connection to Zookeeper
	Severity	Error
	Type	Raise
	Description	Connection to Zookeeper was severed, which might be linked to a Zookeeper down/terminated. Note that a Zookeeper disconnection will cause a Live Data cluster failover.
	Action	Zookeeper is central to Storm and, as such, to Live Data; verify service is up and running. If disconnections are frequent, contact tech. support.
816	Message	[server_id=%s]: Spout Connected Successfully to Zookeeper
	Severity	Informational
	Type	Clear
	Description	Connection to Zookeeper established.
	Action	No action required.
819	Message	[server_id=%s]: Spout deactivated
	Severity	Critical
	Type	Raise
	Description	Event spout is deactivated due to a Live Data Cluster failover. One of the central components to Live Data is down. Central components are: Zookeeper, ActiveMQ, and (pairs of) CCE servers (PG/Router).
	Action	Verify overall system health, i.e., services are up, disk partitions have free space, system is not CPU starved, not swapping, not I/O bound, etc. Verify network to PGs and Routers are healthy. Verify PGs and Routers are up and running. If problem persists, contact tech. support.
820	Message	[server_id=%s]: Spout activated
	Severity	Critical
	Type	Clear
	Description	Event spout transitioned to active state due to startup, or Live Data Cluster failover.
	Action	No action required.

Message ID (decimal)	Property	Value
902	Message	[server_id=%s][value=%s]: Spout UCCE Configuration - Deployment Type Modified
	Severity	Informational
	Type	Clear
	Description	Deployment type change from UCCE to PCCE, or vice-versa. This WILL impact the feature set available in Live Data, and require environment reconfiguration. The expectation is, in fact, that environment adjustments (to/from UCCE to PCCE), took place before changing deployment type.
	Action	No action required.
905	Message	[server_id=%s][value=%s]: Spout UCCE Configuration - Spout end point configuration error
	Severity	Error
	Type	Raise
	Description	Indicates Live Data EndPoint configuration is present, but data is inconsistent (values missing from tables, incomplete data, etc.).
	Action	Correct Live Data EndPoint Configuration.
907	Message	[server_id=%s][value=%s]: Spout UCCE Configuration - Spout TOS end point configuration error
	Severity	Error
	Type	Raise
	Description	Live Data configuration is incomplete/incorrect and TOS protocol host/port is in error.
	Action	Correct Live Data EndPoint Configuration.
1401	Message	[message_error=%s]: Error connecting to Zookeeper
	Severity	Error
	Type	Raise
	Description	Zookeeper connection failure. Possibly Zookeeper service is down, or hung. This will cause Live Data to fail during startup, or to failover if already up.
	Action	Verify overall system health, i.e., services are up, disk partitions have free space, system is not CPU starved, not swapping, not I/O bound, etc. If problem persists, contact tech. support.

Message ID (decimal)	Property	Value
1403	Message	[message_error=%s]: Error communicating with Zookeeper
	Severity	Error
	Type	Raise
	Description	Attempt to write to, or read from, Zookeeper failed, but the error does not characterize Zookeeper to be down. The operation is attempted a few times before the error is reported, so it is very likely Zookeeper connection will be restarted in short order (which will trigger a Live Data Cluster failover).
	Action	Verify overall system health, i.e., services are up, disk partitions have free space, system is not CPU starved, not swapping, not I/O bound, etc. If problem persists, contact tech. support.
1011	Message	[operation_error_desc=%s]: Zookeeper Connection Error
	Severity	Error
	Type	Raise
	Description	Reports error/exception during attempt to connect or operate against Zookeeper instance. Depending on error, a failed connection to Zookeeper is going to be declared, and Live Data Cluster failover will be triggered.
	Action	Verify Zookeeper is up and running. Verify overall system health. If problem persists, contact tech. support.
1014	Message	[value=%s]: Cluster state update
	Severity	Informational
	Type	Clear
	Description	Indicates Live Data Cluster state.
	Action	No action required.
1017	Message	[message_error=%s]: Error in cluster operations
	Severity	Error
	Type	Raise
	Description	Indicates failure during Cluster Peer spout initialization. Also informs failures during TOS request/response and cluster spout stop.
	Action	Verify overall system health. Verify network integrity between Live Data and CCE servers (PG, Router, etc). Verify CCE servers (PG, Router, etc) are up and running. If problem persists, contact tech. support.

Message ID (decimal)	Property	Value
1023	Message	[operation_error_desc=%s]: Cluster Heartbeat subscriber start failed with cause
	Severity	Warning
	Type	Raise
	Description	Cluster Peer Spout failed to initialize JMS (ActiveMQ) subscriber for exchanging of cluster node state, which means cluster failover will not be functional. This can only happen during system startup. JMS (ActiveMQ) configuration is incorrect, or service is down.
	Action	Verify Live Data configuration, verify ActiveMQ service is up and running, and check overall system health. If problem persists, contact tech. support.
1024	Message	Cluster Heartbeat Subscriber started successfully
	Severity	Informational
	Type	Clear
	Description	Cluster Peer Spout successfully connected and subscribed to JMS (ActiveMQ) in order to exchange cluster node state.
	Action	No action required.
1025	Message	[operation_error_desc=%s]: Cluster Publisher start failed with cause
	Severity	Warning
	Type	Raise
	Description	Cluster Peer Spout failed to initialize JMS (ActiveMQ) publisher for exchanging of cluster node state, which means cluster failover will not be functional. This can only happen during system startup. JMS (ActiveMQ) configuration is incorrect, or service is down.
	Action	Verify Live Data configuration, verify ActiveMQ service is up and running, and check overall system health. If problem persists, contact tech. support.
1026	Message	Cluster Publisher started successfully
	Severity	Informational
	Type	Clear
	Description	Cluster Peer Spout successfully connected and can publish to JMS (ActiveMQ) in order to exchange cluster node state.
	Action	No action required.

Message ID (decimal)	Property	Value
1101	Message	[operation_error_desc=%s]: Cluster state machine encounters an error
	Severity	Error
	Type	Raise
	Description	Cluster State Machine is in a state from which received event is invalid!
	Action	Gather logs and contact tech. support.
1107	Message	Cluster state machine activates RTR/PG spouts
	Severity	Informational
	Type	Clear
	Description	Indicates Cluster State Machine has satisfied all conditions to allow for event spouts to connect to CCE servers (PG, Router, etc).
	Action	No action required.
1109	Message	Cluster state machine deactivates RTR/PG spouts
	Severity	Critical
	Type	Raise
	Description	Indicates Cluster State Machine has detected a condition under which event spouts are not allowed to be connected to (or should disconnect from) CCE servers (PG, Router, etc).
	Action	No action required.
1201	Message	[descr=%s]: ActiveMQ connection state down
	Severity	Critical
	Type	Raise
	Description	Indicates ActiveMQ transitioned to down/disconnected state. This will trigger a cluster failover.
	Action	Verify ActiveMQ service is up. Verify network integrity between cluster nodes. Verify overall system health.

Message ID (decimal)	Property	Value
1202	Message	[descr=%s]: ActiveMQ connection state up
	Severity	Critical
	Type	Clear
	Description	Indicates ActiveMQ transitioned to up/connected state.
	Action	No action required.
1301	Message	[descr=Side-%s]: NetBridge connection state down
	Severity	Critical
	Type	Raise
	Description	Indicates ActiveMQ Netbridge transitioned to down/disconnected state. This might trigger a cluster failover depending on TOS request/response to far-end cluster node.
	Action	Verify ActiveMQ service is up. Verify network integrity between cluster nodes. Verify overall system health.
1302	Message	[descr=Side-%s]: NetBridge connection state up
	Severity	Critical
	Type	Clear
	Description	Indicates ActiveMQ Netbridge transitioned to up/connected state.
	Action	No action required.
20101	Message	[db_object_type=%s][message_error=%s]: Error attempting operation with CCE Database
	Severity	Error
	Type	Raise
	Description	Reports database (typically AWDB) runtime error, informing object attempting DB access, and description of failure cause, including SQL query (where appropriate). Failure during connection to AWDB tables to memory, failure to access Hibernate element, failure creating DBSession.
	Action	Determine if AWDB is available, and verify Live Data configuration and CUIC, specifically where it pertains to AWDB connection information on datasource tab in CUIC.

Message ID (decimal)	Property	Value
20103	Message	[message_error=%s]: Error attempting to connect to CCE Database
	Severity	Error
	Type	Raise
	Description	Reports database (typically AWDB) access error during retrieve/update elements, via Hibernate. Execute SQL query, retrieve column value.
	Action	Determine if AWDB is available, and verify Live Data configuration and CUIC, specifically where it pertains to AWDB connection information on datasource tab in CUIC.
20107	Message	[message_error=%s]: Error attempting to read local address from CCE database for Cassandra connection
	Severity	Error
	Type	Raise
	Description	Reports failure during retrieval of configuration element which would allow Live Data a connection to Cassandra DB.
	Action	Verify Live Data configuration.
20201	Message	[db_ver_expected=%s][db_ver_read=%s]: CCE configuration database version mismatch
	Severity	Error
	Type	Raise
	Description	Informs current version found in AWDB is not what Live Data expects to see. This indicates a schema mismatch. Live Data cannot proceed since no data from AWDB can be retrieved. This condition is detected during Live Data startup only.
	Action	Gather logs, and contact tech. support.
20304	Message	Error creating Cassandra Database connection
	Severity	Informational
	Type	Raise
	Description	Reports failure, and cause, during connection attempt to Cassandra DB. Reports Cassandra configuration values used for Cassandra connection.
	Action	Verify Live Data configuration, and assure Cassandra DB is up and running. No action required.

Message ID (decimal)	Property	Value
20305	Message	[message_error=%s]: Error interacting with the Cassandra Connection Pool
	Severity	Error
	Type	Raise
	Description	Reports failure during attempt to obtain connection, from Cassandra connection pool. Most likely connection pool is depleted and new connections to Cassandra DB are not possible.
	Action	Ensure Cassandra DB is up. Verify in Live Data configuration points to Cassandra correctly, and that connection pool is large enough.
20307	Message	[message_error=%s]: Error interacting Cassandra database
	Severity	Error
	Type	Raise
	Description	Reports failure during attempt to read/write to Cassandra DB, and, if available, a description of the problem.
	Action	Ensure Cassandra DB is up, verify Live Data configuration points to Cassandra correctly.
20309	Message	Error reading AWDB Configuration from Cassandra
	Severity	Error
	Type	Raise
	Description	Reports failure, and cause, while reading AWDB Config from Cassandra.
	Action	Verify Live Data configuration, and ensure Cassandra DB is up and running, and AWDBConfig is present using cli "show live-data aw-access"
20401	Message	[message_error=%s]: Error trapped on expected exception
	Severity	Error
	Type	Raise
	Description	Live Data trapped an exception to which it has no recourse other than report and proceed.
	Action	Gather logs and contact tech. support.

Message ID (decimal)	Property	Value
20402	Message	[message_error=%s]: Exception on CCMDB Connection Pool
	Severity	Error
	Type	Raise
	Description	Live Data exception while performing operation on CCM Database connection pool
	Action	Gather logs and contact tech. support.
10703	Message	Tick handler caught a runtime exception
	Severity	Error
	Type	Clear
	Description	The tick handler threw a runtime exception. Scenario Unknown.
	Action	Contact tech. support.
10705	Message	interval processing threw an exception
	Severity	Error
	Type	Clear
	Description	The interval processor threw an exception. Scenario Unknown.
	Action	Contact tech. support.

Live Data TIP Server SNMP Notifications

Table 95: Live Data TIP Server SNMP Notifications

Message ID (hex)	Property	Value
1588001	Message	TIP Server at: %2:%1, failed to start: %3.
	Severity	Error
	Type	Raise
	Description	The TIP Server failed to start. If TIP services are not required, disable TIP in the registry.
	Action	If TIP services are required, configure the proper TIP address/port and restart the node. If TIP services are not required, disable TIP in the registry.

Message ID (hex)	Property	Value
1588002	Message	TIP Server is disabled.
	Severity	Error
	Type	Raise
	Description	The TIP Server has been disabled.
	Action	No action is required.
1588003	Message	TIP Server at: %2:%1, is waiting for client connection.
	Severity	Warning
	Type	Raise
	Description	The TIP Server is waiting for client connections.
	Action	If condition persists, ensure that the Live Data client is running, has connectivity, and the correct configuration information to contact this TIP Server.
1588004	Message	TIP Server at: %3:%1, accepted a connection from:%4:%2.
	Severity	Warning
	Type	Raise
	Description	The TIP Server is waiting for client connections.
	Action	No action is required.
1588006	Message	TIP Server at: %3:%1, client connection: %4:%2, failed: %5.
	Severity	Warning
	Type	Raise
	Description	The TIP Server client connection has failed.
	Action	No action is required.

Message ID (hex)	Property	Value
1588008	Message	TIP Server at: %5:%1, is above warning memory threshold of: %2 MB. Queue will be maintained at: %4; events will be deleted until memory drops below: %3 MB. TIP event loss is possible.
	Severity	Warning
	Type	Raise
	Description	The TIP Server has exceeded configured warning memory limits. The oldest TIP events are being deleted before acknowledgement is received, making event loss possible.
	Action	If this condition persists, ensure that the Live Data client is running, has connectivity and correct configuration information to contact this TIP server.
1588009	Message	TIP Server at: %5:%1, is above critical memory threshold: %2 MB. The queue will be reduced from: %4; events will be deleted until memory drops below: %3 MB. TIP event loss is possible.
	Severity	Error
	Type	Raise
	Description	The TIP Server has exceeded configured critical memory limits. The oldest TIP events are being deleted before acknowledgement is received, making event loss possible.
	Action	If this condition persists, ensure that the Live Data client is running, has connectivity and correct configuration information to contact this TIP Server.
158800A	Message	TIP Server at: %5:%1, is within memory and queue, size limits. Current: %4; events will be kept in queue.
	Severity	Warning
	Type	Raise
	Description	The TIP Server is within configured memory limits.
	Action	None

Message ID (hex)	Property	Value
158800B	Message	TIP Server at: %5:%1, has exceeded maximum: %4; events will be deleted until queue size is reduced. TIP event loss is possible.
	Severity	Warning
	Type	Raise
	Description	The TIP Server has exceeded configured maximum queue size. The oldest TIP events are being deleted before acknowledgement is received, making event loss possible.
	Action	If condition persists, ensure that the Live Data client is running, has connectivity and correct configuration information to contact this TIP Server.
158800C	Message	TIP Server at: %5:%1, has exceeded warning memory threshold: %2 MB, but the queue is below minimum size: %3. The queue may grow at: %4; events will be kept in queue.
	Severity	Warning
	Type	Raise
	Description	The TIP Server has exceeded configured warning memory limits, but has not met the TIP minimum queue size. No action will be taken, but the process may be unstable.
	Action	Monitor process memory usage and take appropriate action if memory overflow is imminent.
158800D	Message	TIP Server at: %5:%1, has exceeded critical memory threshold: %2 MB, but the queue is below minimum size: %3. The queue may grow at: %4; events will be kept in queue.
	Severity	Error
	Type	Raise
	Description	The TIP Server has exceeded configured critical memory limits, but has not met the TIP minimum queue size. No action will be taken, but the process may be unstable.
	Action	Monitor process memory usage and take appropriate action if memory overflow is imminent.

Message ID (hex)	Property	Value
158800E	Message	TIP Server at: %5:%1 has exceeded critical memory threshold: %2 MB; maintaining queue at minimum: %4; events will be deleted until memory drops below: %3 MB. TIP event loss is possible.
	Severity	Error
	Type	Raise
	Description	The TIP Server has exceeded configured critical memory limits. The oldest TIP events are being deleted before acknowledgement is received, making event loss possible.
	Action	Monitor process memory usage and take appropriate action if memory overflow is imminent.
158800F	Message	TIP Server at: %5:%1, has exceeded critical memory threshold: %2 MB, and the queue is below minimum size: %3. The queue will be reduced from: %4. TIP event loss is possible.
	Severity	Error
	Type	Raise
	Description	The TIP Server has exceeded configured critical memory limits, and has not met the TIP minimum queue size. TIP events will be deleted and events may be lost. The process may be unstable.
	Action	Monitor process memory usage and take appropriate action if memory overflow is imminent.

Outbound Option SNMP Notifications

Table 96: Outbound Option SNMP Notifications

Message ID (hex)	Property	Value
1438000	Message	Outbound Option Campaign Manager on: %1, is down.
	Severity	Error
	Type	Raise
	Description	The Outbound Option Campaign Manager is not running. Dialer(s) will only run for a short period of time without a Campaign Manager. In addition, configuration messages will not be forwarded to Dialer(s) or the Import process.
	Action	Make sure the Campaign Manager process is enabled in the registry. Also, check that the Outbound Option database server is running. The Outbound Option private database should have been created with the ICMDBA tool.
1438001	Message	Outbound Option Campaign Manager on: %1, is up.
	Severity	Informational
	Type	Clear
	Description	Outbound Option Campaign Manager is ready to distribute customer records and configuration data.
	Action	No action is required.
1438002	Message	Failed to execute import into table: %1, due to a change in the table's schema.
	Severity	Error
	Type	Single-State Raise
	Description	The schema for a specified table has been changed but the overwrite option has not been enabled. This means that an existing database table does not match the configured import.
	Action	Change the import to an overwrite import. This will drop the existing customer table and create a new table that will match the import. Please note that all existing customer data for that import will be lost.

Message ID (hex)	Property	Value
1438003	Message	Import failed due to an invalid table: %1, definition.
	Severity	Error
	Type	Single-State Raise
	Description	Could not create the specified table due to invalid import schema definition.
	Action	Check that all table columns for the failed import are correct. Making a character column too long could cause this failure.
1438004	Message	Failed to import data into table: %1.
	Severity	Error
	Type	Single-State Raise
	Description	This error could occur if the import file did not match the table definition.
	Action	Check that the import table definition matches the import file.
1438005	Message	Failed to build dialing list from table: %1.
	Severity	Error
	Type	Single-State Raise
	Description	A dialing list could not be populated from the specified table.
	Action	Check if another process has the dialing list table locked. For example, if a report was running on the table while the dialing list was being generated.
1438006	Message	Could not open: %1 database.
	Severity	Error
	Type	Single-State Raise
	Description	The Outbound Option private database has not been initialized or SQL Server is not running.
	Action	Make sure that SQL Server is running. Check the ODBC configuration settings for the Outbound Option private database. Was the ICMDBA tool run to create the Outbound Option private database?

Message ID (hex)	Property	Value
1438007	Message	An import was started but its configuration was deleted while it was running.
	Severity	Error
	Type	Single-State Raise
	Description	An import started running but part of its configuration was deleted before it was able to do anything.
	Action	Reschedule the import.
1438008	Message	Outbound Option CTI Server connection on host: %1 is down.
	Severity	Error
	Type	Raise
	Description	The Outbound Option CTI Server connection has been terminated.
	Action	Make sure CTI Server is active. Also make sure the PIM has connectivity to the switch.
1438009	Message	Outbound Option CTI Server connection on host: %1, is active.
	Severity	Informational
	Type	Clear
	Description	Outbound Option CTI Server connection is active.
	Action	No action is required.
1438010	Message	Dialer telephony port: %1, is not functioning correctly.
	Severity	Error
	Type	Raise
	Description	A telephony error has occurred on a specific Dialer port. This may indicate a fault on the Dialogic telephony card, or the interface card on the switch. However, a more likely scenario is that a T1 line may have been disconnected or cut.
	Action	Check that all wires going to the Dialer and the switch are intact. If port 0 failed, it means the first port on the first telephony card has received a failure message from the telephony driver. The first telephony card is the one that is assigned the lowest ID. The card's ID is assigned by a hardware switch on the top of the card. Ports are numbered consecutively across all ports.

Message ID (hex)	Property	Value
1438011	Message	Outbound Option telephony port: %1, has recovered.
	Severity	Informational
	Type	Clear
	Description	A previously malfunctioning telephony port has received a message from the telephony driver indicating the port is back in service.
	Action	No action is required.
1438012	Message	BAImport is down on host: %1.
	Severity	Error
	Type	Raise
	Description	BAImport is not running on the specified host.
	Action	Please check that the import process has not been shut down. Check that the Outbound Option private database has been created. Also, ensure that SQL Server is running.
1438013	Message	BAImport is up on host: %1.
	Severity	Informational
	Type	Clear
	Description	BAImport is running on the specified host.
	Action	No action is required.
1438014	Message	Dialer is down on host: %1.
	Severity	Error
	Type	Raise
	Description	Dialer is down on the specified host.
	Action	Please check that the Dialogic drivers are configured and running. Also, verify that the Dialer has been started by Node Manager.
1438015	Message	Dialer is up on host: %1.
	Severity	Informational
	Type	Clear
	Description	Dialer is up on the specified host.
	Action	No action is required.

Message ID (hex)	Property	Value
1438018	Message	Failed to rename or delete the import file for import rule ID: %1. This import rule has been temporarily disabled.
	Severity	Error
	Type	Single-State Raise
	Description	Failed to rename or delete the import file for import rule Id: @lt;id; filename@gt;. This import rule has been temporarily disabled. To correct this condition, manually remove the import file and disable and re-enable the import rule using Import Configuration Component.
	Action	File polling is enabled for this import rule. After the import, the BAImport process was unable to rename or delete the file. This import rule is temporarily disabled. Rename or delete the import file, disable and re-enable this import rule from the BAImport Configuration Component.
1438019	Message	Campaign: %1, trying to: %2; database timed out.
	Severity	Error
	Type	Single-State Raise
	Description	Campaign [campaign name] tried to run a query [query name] and the database timed out.
	Action	No action is required.
1438020	Message	Database is running out of space.
	Severity	Error
	Type	Single-State Raise
	Description	Database is running out of space.
	Action	Please create some space in the database.
1438021	Message	The agent skill group: %1, received is not the configured skill group: %2, for the campaign: %3.
	Severity	Error
	Type	Single-State Raise
	Description	The agent skill group received is not configured for this campaign.
	Action	Make sure the skill group configured in the script is the same as the skill group configured in the campaign.

Message ID (hex)	Property	Value
1438022	Message	Timeout happening for the call on port: %1. Time to get the MR response: %2 seconds.
	Severity	Warning
	Type	Single-State Raise
	Description	Timeout happening for the call on port.
	Action	Timeout happening for a call on port. Check the registry key TimeToWaitForMRIResponse.
1438023	Message	Media Routing PIM disconnected with Dialer: %1.
	Severity	Error
	Type	Raise
	Description	Media Routing PIM disconnected with the specified Dialer.
	Action	Check if the MR PIM is active.
1438024	Message	MR PIM connected to Dialer: %1.
	Severity	Error
	Type	Clear
	Description	MR PIM connected to Dialer [dialer name].
	Action	No action is required.
1438025	Message	Import ID: %1, has more than 10,000 errors.
	Severity	Error
	Type	Single-State Raise
	Description	Import process has more than 10,000 errors.
	Action	Restart the import process.
1438026	Message	Dialer: %1, is trying to connect with an incorrect protocol version.
	Severity	Error
	Type	Single-State Raise
	Description	A Dialer with an incorrect protocol version is trying to connect to the Campaign Manager.
	Action	Please check the Dialer version.

Message ID (hex)	Property	Value
1438027	Message	Campaign: %1, DNC list to be imported exceeds the number of DNC records allowed.
	Severity	Error
	Type	Single-State Raise
	Description	The DO Not Call (DNC) list to be imported has exceeded the number of DNC records set by ConfigLimit. Please check the CampaignManager log files for more details.
	Action	Please check the DNC record limit set by the ConfigLimit tool.
1438028	Message	Process: %1; system out of memory.
	Severity	Error
	Type	Single-State Raise
	Description	Memory overflow. Not able to instantiate or assign enough memory.
	Action	This is a memory outage, and the configuration of the system may not be sufficient.
1438029	Message	Dialer: Unknown port owner: %1.
	Severity	Error
	Type	Single-State Raise
	Description	Dialer: Unknown port owner.
	Action	Please check the administrator scripts.
1438030	Message	Cannot find key: %1, in the registry.
	Severity	Error
	Type	Single-State Raise
	Description	Cannot find the specified key in the Windows registry.
	Action	Please ensure that the installation process went smooth.
1438031	Message	Unable to open registry key: %1.
	Severity	Error
	Type	Single-State Raise
	Description	Unable to open registry key.
	Action	Please ensure that the installation process was successful.

Message ID (hex)	Property	Value
1438032	Message	Campaign Manager could not connect to the Outbound Option private database.
	Severity	Error
	Type	Single-State Raise
	Description	Campaign Manager could not connect to the Outbound Option private database.
	Action	Make sure that SQL Server is running and the Outbound Option private database is initialized.
1438033	Message	Dialer attempted to connect to incorrect Campaign Manager version: %1, required version: %2.
	Severity	Error
	Type	Single-State Raise
	Description	Dialer attempted to connect to incorrect Campaign Manager version.
	Action	Please ensure that the Campaign Manager is compatible with the Dialer version.
1438034	Message	Your configured dialer type: %1, doesn't match this dialer type: %2.
	Severity	Error
	Type	Single-State Raise
	Description	Your configured dialer type doesn't match this dialer type.
	Action	Please check the dialer type configured. IP or SIP.
1438035	Message	Dialer has too many ports configured: %1, maximum allowed: %2.
	Severity	Error
	Type	Single-State Raise
	Description	Dialer has too many ports configured.
	Action	Please decrease the number of ports configured.
1438036	Message	Campaign Manager: Unable to convert SystemTime to FileTime.
	Severity	Error
	Type	Single-State Raise
	Description	Internal error: Unable to convert SystemTime to FileTime.
	Action	No action is required.

Message ID (hex)	Property	Value
1438037	Message	Outbound Option connection to SIP server: %1, on host: %2, is down; heartbeat failure detected.
	Severity	Error
	Type	Raise
	Description	Outbound Option SIP server heart beat failure, the connection is down.
	Action	Please make sure SIP server is alive and reachable from Outbound Option SIP dialer.
1438038	Message	Outbound Option connection to SIP server: %1, on host: %2, is up; heartbeat ACK detected.
	Severity	Informational
	Type	Clear
	Description	Outbound Option SIP server heartbeat ACK received, the connection is up.
	Action	No action is required.
1438039	Message	Current private database version is: %1. Required version is: %2.
	Severity	Error
	Type	Single-State Raise
	Description	Outbound Option private database version is not correct. It needs to be upgraded using EDMT.
	Action	Please upgrade private database to the correct version using EDMT for this release.
1438040	Message	Missing/incorrect local static route file is detected on: %1, in the directory: ..\icm\%2\Dialer.
	Severity	Error
	Type	Single-State Raise
	Description	Static route file, ..\Dialer\DNPHost, is missing or has no valid static route entry when configuring the SIP Dialer to connect to voice gateway.
	Action	Re-run the Dialer setup to install sample DNPHost file, and/or enter valid static route entry.

Message ID (hex)	Property	Value
1438041	Message	CPA is disabled on voice gateway: %1; number of calls without CPA: %2.
	Severity	Error
	Type	Single-State Raise
	Description	CPA is disabled or not supported on voice gateway.
	Action	Please enable CPA on voice gateway.
1438042	Message	Action required: Outbound Option database free space is very low: %1%% used.
	Severity	Error
	Type	Single-State Raise
	Description	Outbound Option database space utilization has reached the threshold limit.
	Action	Please increase the database space utilization or remove unnecessary records from the Outbound Option database.
1438043	Message	Skill group: %1, has insufficient records: %2, in the last minute on Dialer: %3.
	Severity	Informational
	Type	Single-State Raise
	Description	Campaign skill group has insufficient customer records.
	Action	Please increase the "records to cache" from the campaign configuration.
1438044	Message	Voice gateway has been overdialed in the the last %1 second(s); resource not available rate is: %2%%; configured-current port throttle: %3.
	Severity	Warning
	Type	Single-State Raise
	Description	The capacity of voice gateway or carrier has been exceeded.
	Action	Please check the capacity of voice gateway or carrier, and adjust the value of "Port Throttle" from the Dialer configuration accordingly.

Message ID (hex)	Property	Value
1438045	Message	SIP Dialer has decreased the port throttle by: %1, since VGW overdialing has been detected in the last %2 seconds; adjusted-configured port throttle: %3.
	Severity	Warning
	Type	Single-State Raise
	Description	SIP Dialer decreases the port throttle since the capacity of voice gateway or carrier is exceeded.
	Action	Please adjust the value of "Port Throttle" from the Dialer configuration or check the Design Guide for the proper sizing calculation for the Outbound Dialer.
1438046	Message	Campaign Manager congestion level changed from: %1 to: %2.
	Severity	Error
	Type	Raise
	Description	There is a change in the congestion level of the Outbound Option Campaign Manager and thus a change in the dialer port throttle percentage. The Campaign Manager will throttle the dialers according to the congestion level, throttling each dialer back to a predetermined percentage of full capacity in order to preserve Campaign Manager throughput and prevent a possible brief outage.
	Action	The Campaign Manager has exceeded its maximum throughput capacity. Re-evaluate the system design if the congestion occurs frequently since the system is not able to maintain the high dialing rate. If congestion is occurring at a dialing rate that was once sustained without congestion, please examine the BA database for fragmentation and/or for a large number of unnecessary rows of data (i.e. please purge unneeded data from the database).
1438047	Message	Campaign Manager congestion level is back to normal.
	Severity	Warning
	Type	Clear
	Description	The Campaign Manager is currently not congested and the dialers have resumed dialing at full capacity.
	Action	None

Message ID (hex)	Property	Value
1438048	Message	Campaign Manager state changed from: %1 to: %2.
	Severity	Warning
	Type	Single-State Raise
	Description	There is a change in the current state of the Outbound Option Campaign Manager. This typically occurs when one Campaign Manager side has failed-over to the peer side. A failover may be due to a failure of the Campaign Manager on one side or due to connectivity issues with the Router, the dialers or the Import process. Only one Campaign Manager will be in an 'active' state at a given time, the other being in a 'standby' state.
	Action	If the state change is not due to an administrator intentionally shutting down the Logger service on the node where the active Campaign Manager is coresident, determine whether the state change is due to a failure of the active Campaign Manager (check the event logs for errors). Lastly, ensure that there are no connectivity issues between the active Campaign Manager and the Router, the Import process or the dialers.
1438059	Message	Imported records count %1 in contact table %2 has reached the threshold of %3
	Severity	Error
	Type	Single-State Raise
	Description	The number of records in the contact table has exceeded the threshold limit, that may in turn be triggered owing to the import being performed without the overwrite option, or the number of records in the import file being large. A large Contact table can result in slow creation of dialing lists as well as excessive space utilization in the BA database
	Action	Run import corresponding to table with overwrite flag enabled or increase the threshold limit.

ICM Network Interface Controller SNMP Notifications

Table 97: ICM Network Interface Controller SNMP Notifications

Message ID (hex)	Property	Value
1288002	Message	SS7 link: %1, in service.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.
1288003	Message	SS7 link: %1, out of service.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the NIC and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the NIC and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	Contact the technical assistance center.
128800A	Message	SS7 linkset: %1, unavailable.
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the NIC and the adjacent signaling point to which the linkset connects.
	Action	Contact the technical assistance center.

Message ID (hex)	Property	Value
128800B	Message	SS7 linkset: %1, available.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset is now available. At least one link in the linkset is operational, although others may still be down. Communication between the NIC and the adjacent signaling point to which the linkset connects has been restored.
	Action	No action is required.
1288101	Message	BTNIC gateway online.
	Severity	Informational
	Type	Clear
	Description	The NIC gateway has entered the online state. The routing client must now be configured, started, and brought online for the NIC to become fully operational. This sequence will proceed automatically.
	Action	No action is required.
1288102	Message	BTNIC gateway stopped: %1.
	Severity	Error
	Type	Raise
	Description	The NIC gateway has stopped operation due to the specified error code. All virtual circuits are blocked. The network should adjust by sending calls to the router through an alternate path utilizing a different NIC. This can be caused by a communication problem between the NIC and the router, by a problem with the router, or by an invalid NIC configuration.
	Action	This event can be caused by a transient problem which may be automatically corrected as indicated by a "gateway online" event. If the problem persists for more than three minutes, the technical assistance center should be alerted to investigate and help correct the problem.
13F8200	Message	Session with client ID: %1, SCP index: %2, configuration valid.
	Severity	Informational
	Type	Clear
	Description	If a configuration error has occurred, it is cleared when the session is closed.
	Action	No action is required.

Message ID (hex)	Property	Value
13F8201	Message	Session with client ID: %1, SCP index: %2, configuration invalid.
	Severity	Error
	Type	Raise
	Description	A problem has occurred with the capabilities or notification masks for this session. Either the mask sent in the open message had undefined bits set or the router requested an action which was not configured in the open session message.
	Action	Determine if the SCP is on line and if the communications links are available.
13F8202	Message	Session with client ID: %1, SCP index: %2, is now open.
	Severity	Informational
	Type	Clear
	Description	A session with the SCP is now open and available to carry traffic.
	Action	No action is required.
13F8203	Message	Session with client ID: %1, SCP index: %2, is now closed.
	Severity	Error
	Type	Raise
	Description	No session is currently opened with the SCP. The SCP index indicates the relative position of that SCP's configuration in the Windows registry.
	Action	Determine if the SCP is on line and if the communications links are available.
13F8206	Message	CRSP GATE online.
	Severity	Informational
	Type	Clear
	Description	The CRSP NIC is online and is prepared to accept route requests from the network.
	Action	No action is required.
13F8207	Message	CRSP GATE offline.
	Severity	Error
	Type	Raise
	Description	The CRSP NIC is offline and cannot accept route requests from the network.
	Action	No action is required.

Message ID (hex)	Property	Value
10D800A	Message	SS7 linkset: %1, unavailable.
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset to the AT&T network is now in a non-working state. This means that all links (usually one, but possibly more) between the NIC and a particular Signal Transfer Point (STP) in the AT&T network are not operational. This is most likely due to a circuit problem in either the Local Exchange Carrier or in the AT&T network. Other possible causes include equipment problems and maintenance procedures. Since the network interface utilizes two linksets, each connected to a different STP, network connectivity is not impacted unless both linksets have failed. If this occurs, a "network inaccessible" alarm will also be generated.
	Action	Occasional brief outages of a single link (and hence a single linkset) are not unusual and require no action. If the outage persists for more than five minutes, or if the outage occurs frequently, contact the AT&T Advanced Features Services Center (AFDSC). Ask to speak to an ICP technician.
10D800B	Message	SS7 linkset: %1, available.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset to the AT&T network is now in a working state.
	Action	No action is required.
10D8010	Message	SS7 network accessible; DPC: %1.
	Severity	Informational
	Type	Clear
	Description	The interface to the AT&T network has returned to a working state. At least one link is now operational, although others may still be down.
	Action	No action is required.

Message ID (hex)	Property	Value
10D8011	Message	SS7 network inaccessible; DPC: %1.
	Severity	Error
	Type	Raise
	Description	All links to the AT&T network from the NIC originating this event are in a non-working state. If the links have not been provisioned with physical diversity, then this outage could arise from a single circuit failure in the Local Exchange Carrier or in the AT&T network. Failure of equipment common to all links is another possible cause, e.g., a T1 multiplexer or electrical power circuit. If you have provisioned a second set of A-links, call routing may still be operational through this alternate path for some or all of your 800 numbers, depending on your network routing configuration. Otherwise, all calls are being default routed.
	Action	Verify that you do not have an equipment failure at your site that could cause this problem. If the outage persists for more than five minutes, or if the outage occurs frequently, contact the AT&T Advanced Features Service Center (AFSC). Ask to speak to an ICP technician. If you have provisioned alternate A-links, use your AT&T network routing application, e.g. Routing Manager, to redirect traffic to the alternate CRP which uses the alternate links.
10D8101	Message	ICP gateway online.
	Severity	Informational
	Type	Clear
	Description	The NIC gateway has entered the online state. The routing client(s) must now be configured, started and brought online for the NIC to become fully operational. This sequence will proceed automatically.
	Action	No action is required.
10D8102	Message	NIC ICP gateway has stopped operation due to the following error: %1. Calls will be default routed.
	Severity	Error
	Type	Raise
	Description	The NIC ICP gateway has stopped operation due to the specified error code. Calls will be default routed. This can be caused by a communication problem between the NIC and the router, by a problem with the router, or by an invalid NIC configuration.
	Action	No action is required.

Message ID (hex)	Property	Value
10D8106	Message	Routing client: %1, stopped: %2.
	Severity	Error
	Type	Raise
	Description	The specified rRouting client has stopped operation for the specified reason code. Calls for the associated subsystem/CRP-ID will be default routed. This can be caused by a communication problem between the NIC and the router, by a problem with the router, or by an invalid NIC configuration.
	Action	This event can be caused by a transient problem which may be automatically corrected. If the problem persists for more than five minutes, contact the technical assistance center.
10D8107	Message	Routing client: %1, online.
	Severity	Informational
	Type	Clear
	Description	The specified routing client is now fully operational and able to process calls for the associated subsystem/CRP-ID.
	Action	No action is required.
1340017	Message	Session for gateway: %1; connect failed to gateway at port: %2 at address: %3.
	Severity	Error
	Type	Raise
	Description	INAP NIC was unable to connect to the gateway on the INAP network.
	Action	Confirm that the gateway is available, that configuration of the IP address and the port are correct, and that network connectivity would allow for connection.
1348009	Message	Gateway: %1, is now accessible.
	Severity	Informational
	Type	Clear
	Description	The INAP NIC has established a communication session with the indicated gateway. This indicates that network connectivity exists to the indicated gateway.
	Action	No action is required.

Message ID (hex)	Property	Value
134800A	Message	Gateway: %1, is no longer accessible.
	Severity	Error
	Type	Raise
	Description	The INAP NIC has disconnected the communication sessions established with the indicated gateway.
	Action	INAP network support should be contacted regarding this problem.
134800C	Message	Gateway: %1, is not accessible.
	Severity	Error
	Type	Raise
	Description	Although connected, the INAP NIC cannot establish a session with the indicated gateway.
	Action	INAP network support should be contacted regarding this problem.
1348200	Message	INAPGATE online.
	Severity	Informational
	Type	Clear
	Description	The INAP NIC is online and is prepared to accept route requests from the INAP network.
	Action	No action is required.
1348201	Message	INAPGATE offline.
	Severity	Error
	Type	Raise
	Description	The INAP NIC is offline and cannot accept route requests from the INAP network.
	Action	No action is required.
1368002	Message	SS7 link: %1; in service.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.

Message ID (hex)	Property	Value
1368003	Message	SS7 link: %1; out of service.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the INAP gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the INAP gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	Contact the technical assistance center.
136800A	Message	SS7 linkset: %1; unavailable.
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the INAP gateway and the adjacent signaling point to which the linkset connects.
	Action	Contact the technical assistance center.
136800B	Message	SS7 linkset: %1; available.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset is now available. At least one link in the linkset is operational, although others may still be down. Communication between the INAP gateway and the adjacent signaling point to which the linkset connects has been restored.
	Action	No action is required.
1368014	Message	SS7 link: %1, of linkset: %2, is in service.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.

Message ID (hex)	Property	Value
1368015	Message	SS7 link: %1, of linkset: %2, is out of service.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the INAP gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the INAP Gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	Contact the technical assistance center.
1368101	Message	INAP gateway online.
	Severity	Informational
	Type	Clear
	Description	The INAP gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.
	Action	No action is required.
1368102	Message	INAP gateway stopped; error: %1.
	Severity	Error
	Type	Raise
	Description	The INAP gateway has stopped operation due to the specified error code. The INAP subsystem is prohibited. The network should adjust by sending calls to the router through an alternate path utilizing a different INAP gateway. This can be caused by a communication problem between the INAP gateway and the NIC, by a problem with the router, or by an administrative INAP gateway command.
	Action	This event can be caused by a transient problem which may be automatically corrected as indicated by a "INAP gateway online" event. If the problem persists for more than three minutes, the technical assistance center should be alerted to help investigate and correct the problem.

Message ID (hex)	Property	Value
1358004	Message	INRCEngine is initiating admission control; device ID: %1.
	Severity	Error
	Type	Raise
	Description	Routing client engine is refusing new calls due to a larger than usual backlog of calls. This may be due to a problem in the router. The routing client engine is now returning overload responses to new call requests and continuing to process existing calls.
	Action	If there is a problem in the router, it may be a transient problem that clears without intervention. If, however, the overload condition does not end within three minutes, as indicated by an "terminating admission control" event, the technical assistance center should be alerted to help investigate and correct the problem.
1358005	Message	INRCEngine is terminating admission control; device ID: %1.
	Severity	Informational
	Type	Clear
	Description	The backlog of calls that caused Admission Control to be initiated has now been reduced to an acceptable level. Usual call routing has resumed.
	Action	No action is required.
135800A	Message	INRCEngine is initiating restriction control for called party: %2; device ID: %1.
	Severity	Warning
	Type	Raise
	Description	Routing client engine is restricting the rate of new calls with the indicated called party number prefix due to a larger than usual backlog of calls.
	Action	No action is required.
135800B	Message	INRCEngine is terminating restriction control on called party: %2; device ID: %1.
	Severity	Informational
	Type	Clear
	Description	Routing client engine is no longer restricting calls with the indicated called party number prefix.
	Action	No action is required.

Message ID (hex)	Property	Value
110800A	Message	MCI RDG: %1 (%2) is now accessible.
	Severity	Informational
	Type	Clear
	Description	The MCI NIC has established its first communication session with the indicated MCI remote data gateway. This indicates that network connectivity exists to the indicated RDG.
	Action	No action is required.
110800B	Message	MCI RDG: %1 (%2) is either out of service or communications between ICM and the RDG has been broken.
	Severity	Error
	Type	Raise
	Description	The MCI NIC no longer has any communication sessions established with the indicated MCI remote data gateway. This points to a problem with the indicated RDG, or a problem with network connectivity.
	Action	The connection between the router and MCI has failed. If all remote data gateways (RDGs) are disconnected from the router then ICM is not routing calls. MCI should be contacted for resolution.
1108200	Message	MCIGATE online.
	Severity	Informational
	Type	Clear
	Description	The MCI NIC is online and is prepared to accept route requests from the MCI network.
	Action	No action is required.
1108201	Message	MCIGATE offline.
	Severity	Error
	Type	Raise
	Description	The MCI NIC is offline and cannot accept route requests from the MCI network.
	Action	No action is required.

Message ID (hex)	Property	Value
12F8009	Message	SCP: %1:%2, is now accessible.
	Severity	Informational
	Type	Clear
	Description	The NORTEL NIC has established a communication session with the indicated SCP. This indicates that network connectivity exists to the indicated SCP.
	Action	No action is required.
12F800A	Message	SCP: %1:%2, is no longer accessible.
	Severity	Error
	Type	Raise
	Description	The NORTEL NIC has disconnected the communication sessions established with the indicated SCP.
	Action	Nortel network support should be contacted regarding this problem.
12F800C	Message	SCP: %1:%2, accessible but session to other side SCP: %1:%3, is still active.
	Severity	Informational
	Type	Clear
	Description	The NORTEL NIC has established a communication session with the indicated SCP and side while a session to the other side of the SCP is still active. This indicates that a failover situation to the SCP has occurred.
	Action	Determine cause of failover.
12F8200	Message	NTGATE is online.
	Severity	Informational
	Type	Clear
	Description	The NORTEL NIC is online and is prepared to accept route requests from the Nortel network.
	Action	No action is required.

Message ID (hex)	Property	Value
12F8201	Message	NTGATE is offline.
	Severity	Error
	Type	Raise
	Description	The NORTEL NIC is offline and cannot accept route requests from the Nortel network.
	Action	No action is required.
1420017	Message	Session for gateway: %1, connect failed to gateway at port: %2, address: %3.
	Severity	Error
	Type	Raise
	Description	CWC NIC was unable to connect to the gateway on the CWC network.
	Action	Confirm gateway is available, configuration of IP address and port are correct, and network connectivity would allow for connection.
1428009	Message	Gateway: %1, is now accessible.
	Severity	Informational
	Type	Clear
	Description	The CWC NIC has established a communication session with the indicated gateway. This indicates that network connectivity exists to the indicated gateway.
	Action	No action is required.
142800A	Message	Gateway: %1, is no longer accessible.
	Severity	Error
	Type	Raise
	Description	The CWC NIC has disconnected the communication sessions established with the indicated gateway.
	Action	CWC network support should be contacted regarding this problem.

Message ID (hex)	Property	Value
142800C	Message	Gateway: %1, is not accessible.
	Severity	Error
	Type	Raise
	Description	Although connected, the CWC NIC cannot establish a session with the indicated gateway.
	Action	CWC network support should be contacted regarding this problem.
1428200	Message	C&W NIC routing client is online.
	Severity	Informational
	Type	Clear
	Description	The CWC NIC is online and is prepared to accept route requests from the CWC network.
	Action	No action is required.
1428201	Message	C&W NIC routing client is offline.
	Severity	Error
	Type	Raise
	Description	The CWC NIC is offline and cannot accept route requests from the CWC network.
	Action	No action is required.
1428203	Message	SS7 link: %1, in service.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.

Message ID (hex)	Property	Value
1428204	Message	SS7 link: %1, out of service.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the INAP gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the INAP gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	Contact the technical assistance center.
142820B	Message	SS7 linkset: %1, unavailable.
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the INAP Gateway and the adjacent signaling point to which the linkset connects.
	Action	Contact the technical assistance center.
142820C	Message	SS7 linkset: %1, available.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset is now available. At least one link in the linkset is operational, although others may still be down. Communication between the INAP Gateway and the adjacent signaling point to which the linkset connects has been restored.
	Action	No action is required.
1428210	Message	INAP gateway online.
	Severity	Informational
	Type	Clear
	Description	The INAP gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.
	Action	No action is required.

Message ID (hex)	Property	Value
1428211	Message	INAP gateway stopped: %1.
	Severity	Error
	Type	Raise
	Description	The INAP gateway has stopped operation due to the specified error code. The INAP subsystem is prohibited. The network should adjust by sending calls to the router through an alternate path utilizing a different INAP gateway. This can be caused by a communication problem between the INAP Gateway and the NIC, by a problem with the router, or by an administrative INAP gateway command.
	Action	This event can be caused by a transient problem which may be automatically corrected as indicated by a "INAP gateway online" event. If the problem persists for more than three minutes, the technical assistance center should be alerted to investigate and help correct the problem.
1428310	Message	SS7 link is out of service (Gateway PC: %1, Linkset RPC: %2, Link SLC: %3) (%4).
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the SS7 gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the SS7 gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	No action is required.
1428311	Message	SS7 link is in service (Gateway PC: %1, Linkset RPC: %2, Link SLC: %3).
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.

Message ID (hex)	Property	Value
1428312	Message	SS7 linkset unavailable (Gateway PC: %1, Linkset RPC: %2) .
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the SS7 gateway and the adjacent signaling point to which the linkset connects.
	Action	Contact the technical assistance center.
1428313	Message	SS7 linkset available (Gateway PC: %1, Linkset RPC: %2) .
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset is now available. At least one link in the linkset is operational, although others may still be down. Communication between the SS7 gateway and the adjacent signaling point to which the linkset connects has been restored.
	Action	No action is required.
1460017	Message	Session for gateway: %1, connect failed to gateway: port: %2, address: %3.
	Severity	Error
	Type	Raise
	Description	Unisource NIC was unable to connect to the gateway on the Unisource network.
	Action	Confirm gateway is available, configuration of IP address and port are correct, and network connectivity would allow for connection.
1468009	Message	Gateway: %1, is now accessible.
	Severity	Informational
	Type	Clear
	Description	The Unisource NIC has established a communication session with the indicated gateway. This indicates that network connectivity exists to the indicated gateway.
	Action	No action is required.

Message ID (hex)	Property	Value
146800A	Message	Gateway: %1, is no longer accessible.
	Severity	Error
	Type	Raise
	Description	The Unisource NIC has disconnected the communication sessions established with the indicated gateway.
	Action	Unisource network support should be contacted regarding this problem.
146800B	Message	Gateway: %1, is not accessible.
	Severity	Error
	Type	Raise
	Description	Although connected, the Unisource NIC cannot establish a session with the indicated gateway.
	Action	Unisource network support should be contacted regarding this problem.
146800D	Message	SS7 link: %1, in service.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.
146800E	Message	SS7 link: %1, out of service.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the SS7 gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the SS7 gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	Contact the technical assistance center.

Message ID (hex)	Property	Value
1468015	Message	SS7 linkset: %1, unavailable.
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the SS7 gateway and the adjacent signaling point to which the linkset connects.
	Action	Contact the technical assistance center.
1468016	Message	SS7 linkset: %1, available.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset is now available. At least one link in the linkset is operational, although others may still be down. Communication between the SS7 gateway and the adjacent signaling point to which the linkset connects has been restored.
	Action	No action is required.
1468017	Message	SS7 gateway online.
	Severity	Informational
	Type	Clear
	Description	The SS7 gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.
	Action	No action is required.
1468018	Message	SS7 gateway stopped: %1.
	Severity	Error
	Type	Raise
	Description	The SS7 gateway has stopped operation due to the specified error code. The SS7 subsystem is prohibited. The network should adjust by sending calls to the Router through an alternate path utilizing a different SS7 gateway. This can be caused by a communication problem between the SS7 gateway and the NIC, by a problem with the Router, or by an administrative SS7 gateway command.
	Action	This event can be caused by a transient problem which may be automatically corrected as indicated by an "SS7 gateway online" event. If the problem persists for more than three minutes, the technical assistance center should be alerted to help investigate and correct the problem.

Message ID (hex)	Property	Value
1468200	Message	UNISOURCE routing client is online.
	Severity	Informational
	Type	Clear
	Description	The Unisource NIC is online and is prepared to accept route requests from the Unisource network.
	Action	No action is required.
1468201	Message	UNISOURCE routing client is offline.
	Severity	Error
	Type	Raise
	Description	The Unisource NIC is offline and cannot accept route requests from the Unisource network.
	Action	No action is required.
1468310	Message	SS7 link is out of service (gateway PC: %1, linkset RPC: %2, link SLC: %3): %4.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the SS7 gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the SS7 gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	No action is required.
1468311	Message	SS7 link is in service (gateway PC: %1, linkset RPC: %2, link SLC: %3).
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.

Message ID (hex)	Property	Value
1468312	Message	SS7 linkset unavailable (gateway PC: %1, linkset RPC: %2) .
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the SS7 gateway and the adjacent signaling point to which the linkset connects.
	Action	Contact the technical assistance center.
1468313	Message	SS7 linkset available (gateway PC: %1, linkset RPC: %2) .
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset is now available. At least one link in the linkset is operational, although others may still be down. Communication between the SS7 gateway and the adjacent signaling point to which the linkset connects has been restored.
	Action	No action is required.
1468314	Message	SCTP connection is down (connection number: %1, remote entity: %2) .
	Severity	Error
	Type	Raise
	Description	The SCTP association to the remote entity is down. Communication has failed and calls cannot be processed through this connection. Check the gateway logs for configuration errors and/or check the remote entity.
	Action	No action is required.
1468315	Message	ASP is down (connection number: %1, remote entity: %2) .
	Severity	Error
	Type	Raise
	Description	The SCTP association to the remote entity is established, but the ASP is down. Calls cannot be processed through this connection. Check the gateway logs for configuration errors and/or check the remote entity.
	Action	No action is required.

Message ID (hex)	Property	Value
1468316	Message	ASP is inactive (connection number: %1, remote entity: %2) .
	Severity	Error
	Type	Raise
	Description	The ASP is up, but is not yet active. Calls cannot be processed through this connection. Check the gateway logs for configuration errors and/or check the remote entity.
	Action	No action is required.
1468317	Message	ASP is active (connection number: %1, remote entity: %2) .
	Severity	Informational
	Type	Clear
	Description	The ASP is active. Calls can be processed through this connection.
	Action	No action is required.
1490017	Message	Session for gateway: %1, connect failed to gateway at port: %2, at address: %3.
	Severity	Error
	Type	Raise
	Description	CONCERT NIC was unable to connect to the gateway on the CONCERT network.
	Action	Confirm gateway is available, configuration of IP address and port are correct, and network connectivity would allow for connection
1498009	Message	Gateway: %1, is now accessible.
	Severity	Informational
	Type	Clear
	Description	The CONCERT NIC has established a communication session with the indicated gateway. This indicates that network connectivity exists to the indicated gateway.
	Action	No action is required.

Message ID (hex)	Property	Value
149800A	Message	Gateway: %1, is no longer accessible.
	Severity	Error
	Type	Raise
	Description	The CONCERT NIC has disconnected the communication sessions established with the indicated gateway.
	Action	CONCERT network support should be contacted regarding this problem.
149800C	Message	Gateway: %1, is not accessible.
	Severity	Error
	Type	Raise
	Description	Although connected, the CONCERT NIC cannot establish a session with the indicated gateway.
	Action	CONCERT network support should be contacted regarding this problem.
1498200	Message	CONCERTGATE online.
	Severity	Informational
	Type	Clear
	Description	The CONCERT NIC is online and is prepared to accept route requests from the CONCERT network.
	Action	No action is required.
1498201	Message	CONCERTGATE offline.
	Severity	Error
	Type	Raise
	Description	The CONCERT NIC is offline and cannot accept route requests from the CONCERT network.
	Action	No action is required.
1498203	Message	SS7 link: %1, in service.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.

Message ID (hex)	Property	Value
1498204	Message	SS7 link: %1, out of service.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the INAP gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the INAP gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	Contact the technical assistance center.
149820B	Message	SS7 linkset: %1, unavailable.
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the INAP gateway and the adjacent signaling point to which the linkset connects.
	Action	Contact the technical assistance center.
149820C	Message	SS7 linkset: %1, available.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset is now available. At least one link in the linkset is operational, although others may still be down. Communication between the INAP gateway and the adjacent signaling point to which the linkset connects has been restored.
	Action	No action is required.
1498210	Message	INAP gateway online.
	Severity	Informational
	Type	Clear
	Description	The INAP gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.
	Action	No action is required.

Message ID (hex)	Property	Value
1498211	Message	INAP gateway stopped: %1.
	Severity	Error
	Type	Raise
	Description	The INAP gateway has stopped operation due to the specified error code. The INAP subsystem is prohibited. The network should adjust by sending calls to the router through an alternate path utilizing a different INAP gateway. This can be caused by a communication problem between the INAP gateway and the NIC, by a problem with the router, or by an administrative INAP gateway command.
	Action	This event can be caused by a transient problem which may be automatically corrected as indicated by a "INAP gateway online" event. If the problem persists for more than three minutes, the technical assistance center should be alerted to investigate and help correct the problem.
14C0017	Message	Session for gateway: %1, connect failed to gateway at port: %2, at address: %3.
	Severity	Error
	Type	Raise
	Description	BT-V2 INAP NIC was unable to connect to the gateway on the INAP network.
	Action	Confirm gateway is available, configuration of IP address and port are correct, and network connectivity would allow for connection.
14C8009	Message	Gateway: %1, is now accessible.
	Severity	Informational
	Type	Clear
	Description	The BT-V2 INAP NIC has established a communication session with the indicated gateway. This indicates that network connectivity exists to the indicated gateway.
	Action	No action is required.
14C800A	Message	Gateway: %1, is no longer accessible.
	Severity	Error
	Type	Raise
	Description	The BT-V2 INAP NIC has disconnected the communication sessions established with the indicated gateway.
	Action	INAP network support should be contacted regarding this problem.

Message ID (hex)	Property	Value
14C800C	Message	Gateway: %1, is not accessible.
	Severity	Error
	Type	Raise
	Description	Although connected, the BT-V2 INAP NIC cannot establish a session with the indicated gateway.
	Action	INAP network support should be contacted regarding this problem.
14C8200	Message	BT-V2 NIC routing client is online.
	Severity	Informational
	Type	Clear
	Description	The BT-V2 INAP NIC is online and is prepared to accept route requests from the INAP network.
	Action	No action is required.
14C8201	Message	BT-V2 NIC routing client is offline.
	Severity	Error
	Type	Raise
	Description	The BT-V2 INAP NIC is offline and cannot accept route requests from the INAP network.
	Action	No action is required.
14C8203	Message	SS7 link: %1, in service.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.

Message ID (hex)	Property	Value
14C8204	Message	SS7 link: %1, out of service.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the INAP Gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the INAP Gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	Contact the technical assistance center.
14C820B	Message	SS7 linkset: %1, unavailable.
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the INAP Gateway and the adjacent signaling point to which the linkset connects.
	Action	Contact the technical assistance center.
14C820C	Message	SS7 linkset: %1, available.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset is now available. At least one link in the linkset is operational, although others may still be down. Communication between the INAP gateway and the adjacent signaling point to which the linkset connects has been restored.
	Action	No action is required.
14C8210	Message	INAP gateway online.
	Severity	Informational
	Type	Clear
	Description	The INAP gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.
	Action	No action is required.

Message ID (hex)	Property	Value
14C8211	Message	INAP gateway stopped: %1.
	Severity	Error
	Type	Raise
	Description	The INAP gateway has stopped operation due to the specified error code. The INAP subsystem is prohibited. The network should adjust by sending calls to the router through an alternate path utilizing a different INAP gateway. This can be caused by a communication problem between the INAP gateway and the NIC, by a problem with the Router, or by an administrative INAP gateway command.
	Action	This event can be caused by a transient problem which may be automatically corrected as indicated by a "INAP gateway ONLINE" event. If the problem persists for more than three minutes, the technical assistance center should be alerted to investigate and help correct the problem.
14C8310	Message	SS7 link is out of service: gateway PC: %1, linkset RPC: %2, link SLC: %3; %4.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the SS7 gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the SS7 gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	No action is required.
14C8311	Message	SS7 link is in service: gateway PC: %1, linkset RPC: %2, link SLC: %3.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.

Message ID (hex)	Property	Value
14C8312	Message	SS7 linkset unavailable: gateway PC: %1, linkset RPC: %2.
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the SS7 gateway and the adjacent signaling point to which the linkset connects.
	Action	Contact the technical assistance center.
14C8313	Message	SS7 linkset available: gateway PC; %1, linkset RPC: %2.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset is now available. At least one link in the linkset is operational, although others may still be down. Communication between the SS7 gateway and the adjacent signaling point to which the linkset connects has been restored.
	Action	No action is required.
14D0017	Message	Session for gateway: %1, connect failed to gateway: port: %2, address: %3.
	Severity	Error
	Type	Raise
	Description	TIM NIC was unable to connect to the gateway on the INAP network.
	Action	Confirm gateway is available, configuration of IP address and port are correct, and network connectivity would allow for connection.
14D8009	Message	Gateway: %1, is now accessible.
	Severity	Informational
	Type	Clear
	Description	The TIM NIC has established a communication session with the indicated gateway. This indicates that network connectivity exists to the indicated gateway.
	Action	No action is required.

Message ID (hex)	Property	Value
14D800A	Message	Gateway: %1, is no longer accessible.
	Severity	Error
	Type	Raise
	Description	The TIM NIC has disconnected the communication sessions established with the indicated gateway.
	Action	INAP network support should be contacted regarding this problem.
14D800C	Message	Gateway: %1, is not accessible.
	Severity	Error
	Type	Raise
	Description	Although connected, the TIM NIC cannot establish a session with the indicated gateway.
	Action	INAP network support should be contacted regarding this problem.
14D8200	Message	TIM NIC routing client is online.
	Severity	Informational
	Type	Clear
	Description	The TIM NIC is online and is prepared to accept route requests from the INAP network.
	Action	No action is required.
14D8201	Message	TIM NIC routing client is offline.
	Severity	Error
	Type	Raise
	Description	The TIM NIC is offline and cannot accept route requests from the INAP network.
	Action	No action is required.
14D8203	Message	SS7 link: %1, in service.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.

Message ID (hex)	Property	Value
14D8204	Message	SS7 link: %1, out of service.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the INAP gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the INAP gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	Contact the technical assistance center.
14D820B	Message	SS7 linkset: %1, unavailable.
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the INAP gateway and the adjacent signaling point to which the linkset connects.
	Action	Contact the technical assistance center.
14D820C	Message	SS7 linkset: %1, available.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset is now available. At least one link in the linkset is operational, although others may still be down. Communication between the INAP gateway and the adjacent signaling point to which the linkset connects has been restored.
	Action	No action is required.
14D8210	Message	INAP gateway online.
	Severity	Informational
	Type	Clear
	Description	The INAP gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.
	Action	No action is required.

Message ID (hex)	Property	Value
14D8211	Message	INAP gateway stopped: %1.
	Severity	Error
	Type	Raise
	Description	The INAP gateway has stopped operation due to the specified error code. The INAP subsystem is prohibited. The network should adjust by sending calls to the Router through an alternate path utilizing a different INAP gateway. This can be caused by a communication problem between the INAP gateway and the NIC, by a problem with the Router, or by an administrative INAP gateway command.
	Action	This event can be caused by a transient problem which may be automatically corrected as indicated by a "INAP gateway online" event. If the problem persists for more than three minutes, the technical assistance center should be alerted to investigate and correct the problem.
14D8310	Message	SS7 link is out of service (gateway PC: %1, linkset RPC: %2, link SLC: %3): %4.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the SS7 gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the SS7 gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	No action is required.
14D8311	Message	SS7 link is in service (gateway PC: %1, linkset RPC: %2, link SLC: %3).
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.

Message ID (hex)	Property	Value
14D8312	Message	SS7 linkset unavailable (gateway PC: %1, linkset RPC: %2) .
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the SS7 gateway and the adjacent signaling point to which the linkset connects.
	Action	Contact the technical assistance center.
14D8313	Message	SS7 linkset available (gateway PC: %1, linkset RPC: %2) .
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset is now available. At least one link in the linkset is operational, although others may still be down. Communication between the SS7 gateway and the adjacent signaling point to which the linkset connects has been restored.
	Action	No action is required.
14D8314	Message	SCTP connection is down (connection number: %1, remote entity: %2) .
	Severity	Error
	Type	Raise
	Description	The SCTP Association to the remote entity is down. Communication has failed and calls cannot be processed through this connection. Check the gateway logs for configuration errors and/or check the remote entity.
	Action	No action is required.
14D8315	Message	ASP is down (connection number: %1, remote entity: %2) .
	Severity	Error
	Type	Raise
	Description	The SCTP association to the remote entity is established, but the ASP is down. Calls cannot be processed through this connection. Check the gateway logs for configuration errors and/or check the remote entity.
	Action	No action is required.

Message ID (hex)	Property	Value
14D8316	Message	ASP is inactive (connection number: %1, remote entity: %2) .
	Severity	Error
	Type	Raise
	Description	The ASP is up, but is not yet active. Calls cannot be processed through this connection. Check the gateway logs for configuration errors and/or check the remote entity.
	Action	No action is required.
14D8317	Message	ASP is active (connection number: %1, remote entity: %2) .
	Severity	Informational
	Type	Clear
	Description	The ASP is active. Calls can be processed through this connection.
	Action	No action is required.
14F0017	Message	Session for gateway: %1, connect failed to SS7 gateway; port: %2, address: %3.
	Severity	Error
	Type	Raise
	Description	SS7 IN NIC was unable to connect to the SS7 gateway.
	Action	Confirm SS7 gateway is available, configuration of IP address and port are correct, and network connectivity would allow for connection.
14F8009	Message	SS7 gateway: %1, is now accessible.
	Severity	Informational
	Type	Clear
	Description	The SS7 IN NIC has established a communication session with the SS7 gateway. This confirms that network connectivity exists to the indicated SS7 gateway.
	Action	No action is required.

Message ID (hex)	Property	Value
14F800A	Message	SS7 gateway: %1, is no longer accessible.
	Severity	Error
	Type	Raise
	Description	The SS7 IN NIC has disconnected the communication sessions established with the indicated SS7 gateway.
	Action	SS7 network support should be contacted regarding this problem.
14F800C	Message	SS7 gateway: %1, is not accessible.
	Severity	Error
	Type	Raise
	Description	Although connected, the SS7 IN NIC cannot establish a session with the indicated gateway.
	Action	SS7 network support should be contacted regarding this problem.
14F8102	Message	SS7 link: %1, in service.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.
14F8103	Message	SS7 link: %1, out of service.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the SS7 gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the SS7 gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	Contact the technical assistance center.

Message ID (hex)	Property	Value
14F810A	Message	SS7 linkset: %1, unavailable.
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the SS7 gateway and the adjacent signaling point to which the linkset connects.
	Action	Contact the technical assistance center.
14F810B	Message	SS7 linkset: %1, available.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset is now available. At least one link in the linkset is operational, although others may still be down. Communication between the SS7 gateway and the adjacent signaling point to which the linkset connects has been restored.
	Action	No action is required.
14F8114	Message	SS7 link: %1, of linkset: %2, is in service.
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.
14F8115	Message	SS7 link: %1, of linkset: %2, is out of service.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the SS7 gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the SS7 gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	Contact the technical assistance center.

Message ID (hex)	Property	Value
14F8310	Message	SS7 link is out of service (gateway PC: %1, linkset RPC: %2, link SLC: %3): %4.
	Severity	Error
	Type	Raise
	Description	The specified SS7 link is now out of service. This is most likely due to a circuit problem between the SS7 gateway and the adjacent signaling point to which this link connects. Equipment problems are also a possible cause. Because each link typically belongs to a linkset containing two or more links, connectivity between the SS7 gateway and the adjacent signaling point is not lost unless all other links in the linkset have failed. If this occurs, a "linkset unavailable" alarm is generated.
	Action	No action is required.
14F8311	Message	SS7 link is in service (gateway PC: %1, linkset RPC: %2, link SLC: %3).
	Severity	Informational
	Type	Clear
	Description	The specified SS7 link is now aligned and in service.
	Action	No action is required.
14F8312	Message	SS7 linkset unavailable (gateway PC: %1, linkset RPC: %2).
	Severity	Error
	Type	Raise
	Description	The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the SS7 gateway and the adjacent signaling point to which the linkset connects.
	Action	Contact the technical assistance center.
14F8313	Message	SS7 linkset available (gateway PC: %1, linkset RPC: %2).
	Severity	Informational
	Type	Clear
	Description	The specified SS7 linkset is now available. At least one link in the linkset is operational, although others may still be down. Communication between the SS7 gateway and the adjacent signaling point to which the linkset connects has been restored.
	Action	No action is required.

Message ID (hex)	Property	Value
14F8314	Message	SCTP connection is down (connection number: %1, remote entity: %2).
	Severity	Error
	Type	Raise
	Description	The SCTP Association to the remote entity is down. Communication has failed and calls cannot be processed through this connection. Check the gateway logs for configuration errors and/or check the remote entity.
	Action	No action is required.
14F8315	Message	ASP is down (connection number: %1, remote entity: %2).
	Severity	Error
	Type	Raise
	Description	The SCTP association to the remote entity is established, but the ASP is down. Calls cannot be processed through this connection. Check the gateway logs for configuration errors and/or check the remote entity.
	Action	No action is required.
14F8316	Message	ASP is inactive (connection number: %1, remote entity: %2).
	Severity	Error
	Type	Raise
	Description	The ASP is up, but is not yet active. Calls cannot be processed through this connection. Check the gateway logs for configuration errors and/or check the remote entity.
	Action	No action is required.
14F8317	Message	ASP is active (connection number: %1, remote entity: %2).
	Severity	Informational
	Type	Clear
	Description	The ASP is active. Calls can be processed through this connection.
	Action	No action is required.

Message ID (hex)	Property	Value
1504001	Message	The NTL NIC received an invalid label: %1. from the router for the call (tid: %2).
	Severity	Error
	Type	Application Error
	Description	The NTL NIC received an invalid label from the router. Check the label format and size.
	Action	Check labels in the label table for invalid labels.
1508006	Message	Starting NTL network communications.
	Severity	Informational
	Type	Clear
	Description	The network communication layer of the NTL NIC is starting operation.
	Action	No action is required.
1508007	Message	Stopping NTL network communications.
	Severity	Warning
	Type	Raise
	Description	The network communication layer of the NTL NIC is halting operation.
	Action	No action is required.
1508009	Message	Starting a NTL communication channel: %1, with CE: %4:%2.
	Severity	Informational
	Type	Clear
	Description	A communication channel of the NTL NIC is starting operation.
	Action	No action is required.
150800A	Message	Stopping the NTL communication channel: %1, to CE: %4:%2.
	Severity	Error
	Type	Raise
	Description	A communication channel of the NTL NIC is halting operation.
	Action	No action is required.

Message ID (hex)	Property	Value
150800B	Message	Closing the NTL communication channel: %1, by CE: %4:%2.
	Severity	Error
	Type	Raise
	Description	A communication channel of the NTL NIC is closed by the SCP.
	Action	No action is required.

TDM Peripheral Gateway SNMP Notifications

Table 98: TDM Peripheral Gateway SNMP Notifications

Message ID (hex)	Property	Value
1530002	Message	A required parameter is invalid.
	Severity	Error
	Type	Raise
	Description	One or more of the required parameters are invalid.
	Action	Internal error. Contact the technical assistance center.
1530015	Message	One or more ICM/AW connection parameters are null or empty.
	Severity	Error
	Type	Raise
	Description	One or more required ICM/AW connection parameters are null or empty.
	Action	Make sure that all required ICM/AW connection information exists in the registry and is correct (see Troubleshooting Guide). If the information is in the registry and is correct, contact technical support.
1530017	Message	Fatal connection error to ICM/AW.
	Severity	Error
	Type	Raise
	Description	All retry and failover attempts to the ICM AW(s) have failed.
	Action	See the AAS Installation and Troubleshooting Guide for information on correcting ICM/AW connection errors.

Message ID (hex)	Property	Value
1530018	Message	ICM/AW authentication failed.
	Severity	Error
	Type	Raise
	Description	AAS is unable to log into the ICM/AW because the login authentication failed.
	Action	Check login information in the registry (see Troubleshooting Guide) and make sure it matches the login information used to setup the application on the ICM/AW.
1530019	Message	Unable to retrieve a PG name from the peripheral table.
	Severity	Error
	Type	Raise
	Description	Unable to retrieve a PG name from the peripheral table.
	Action	Make sure a PG Name is configured for the peripheral that is set up for AAS.
153001A	Message	Error adding record to ICM/AW.
	Severity	Error
	Type	Raise
	Description	AAS was unable to add a record to the ICM/AW. A possible reason is that the ICM/AW is out of sync with Symposium.
	Action	Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).
153001B	Message	Error deleting record from ICM/AW.
	Severity	Error
	Type	Raise
	Description	AAS was unable to delete a record from ICM/AW. A possible reason is that the ICM/AW is out of sync with Symposium.
	Action	Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).

Message ID (hex)	Property	Value
153001C	Message	Error updating record in ICM/AW.
	Severity	Error
	Type	Raise
	Description	AAS was unable to update a record in ICM/AW. A possible reason is that the ICM/AW is out of sync with Symposium.
	Action	Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).
153001D	Message	Error performing bulk update of the ICM/AW.
	Severity	Error
	Type	Raise
	Description	AAS was unable to perform a bulk update of the ICM/AW. A possible reason is that the ICM/AW is out of sync with Symposium.
	Action	Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).
153001E	Message	Bad ICM/AW operation type used.
	Severity	Error
	Type	Raise
	Description	A bad ICM/AW operation type was used. Update, delete, insert, and destroy permanently are the only operation types supported.
	Action	Internal error. Contact the technical assistance center.
153001F	Message	Lost connection to the ICM/AW.
	Severity	Error
	Type	Raise
	Description	AAS lost its connection to the ICM/AW due to an unknown cause.
	Action	AAS should self-correct. If it does not, consult the AAS Installation and Troubleshooting Guide for information on correcting connection errors to ICM.

Message ID (hex)	Property	Value
1530020	Message	Error retrieving records from the ICM/AW.
	Severity	Error
	Type	Raise
	Description	AAS was unable to retrieve records from the ICM/AW. A possible reason is that the ICM/AW is out of sync with Symposium.
	Action	Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).
1530021	Message	Error retrieving peripheral record from ICM/AW.
	Severity	Error
	Type	Raise
	Description	AAS was unable to retrieve a peripheral record from ICM/AW. The record was not created in the ICM/AW or the ID for it was not set properly in the registry.
	Action	Make sure a peripheral is set up in the ICM/AW for AAS. Ensure the peripheral ID is properly configured in the AAS configuration registry (see Troubleshooting Guide).
1530022	Message	Error retrieving skill group from ICM/AW.
	Severity	Error
	Type	Raise
	Description	AAS was unable to retrieve a skill group from ICM/AW. A possible reason is that the ICM/AW is out of sync with Symposium.
	Action	Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).
1530023	Message	Agent priority specified is beyond maximum allowed limits.
	Severity	Error
	Type	Raise
	Description	The agent priority specified was configured with a priority greater than the maximum allowed limit of 48.
	Action	Internal error. Contact the technical assistance center.

Message ID (hex)	Property	Value
1530033	Message	Config services requested before config info set.
	Severity	Error
	Type	Raise
	Description	Configuration services were requested before the configuration information was set up.
	Action	Internal error. Contact the technical assistance center.
1530034	Message	An unexpected key type was given to the config service.
	Severity	Error
	Type	Raise
	Description	A configuration parameter for AAS was setup with the wrong key type in the registry.
	Action	Recreate the key with the proper type (see Troubleshooting Guide).
15301F4	Message	AAS disconnected from the ICM/AW.
	Severity	Informational
	Type	Raise
	Description	AAS disconnected from the ICM/AW.
	Action	AAS should reset its connection to ICM. If it doesn't, restart AAS.
15301F6	Message	Connection to the ICM/AW established.
	Severity	Informational
	Type	Clear
	Description	The connection between AAS and the ICM/AW has been established.
	Action	No action is required.
1530051	Message	Configuration given to MasterSelection is null.
	Severity	Error
	Type	Raise
	Description	MasterSelection cannot start because the AAS PG hosts and ports were not configured in the registry.
	Action	Correct registry data for AASPG Hosts and Ports (see Troubleshooting Guide).

Message ID (hex)	Property	Value
1530052	Message	Bad IP address for side A MasterSelection.
	Severity	Error
	Type	Raise
	Description	The configuration IP address for the side A MasterSelection is badly formed or cannot be found.
	Action	Correct the AASPGHostA and AASPGPortA configuration data in the registry (see Troubleshooting Guide).
1530053	Message	Bad IP address for side B MasterSelection.
	Severity	Error
	Type	Raise
	Description	The configuration IP address for the side B MasterSelection is badly formed or cannot be found.
	Action	Correct the AASPGHostB and AASPGPortB configuration data in the registry (see Troubleshooting Guide).
1530054	Message	Null IP address for side A MasterSelection.
	Severity	Error
	Type	Raise
	Description	The configuration IP address for the side A MasterSelection is blank, which is not allowed.
	Action	Correct the AASPGHostA and AASPGPortA configuration data in the registry (see Troubleshooting Guide).
1530055	Message	Null IP address for side B MasterSelection.
	Severity	Error
	Type	Raise
	Description	The configuration IP address for the side B MasterSelection is blank, which is not allowed.
	Action	Correct the AASPGHostB and AASPGPortB configuration data in the registry (see Troubleshooting Guide).

Message ID (hex)	Property	Value
1530056	Message	Bind exception or socket exception trying to open socket for MasterSelection.
	Severity	Error
	Type	Raise
	Description	MasterSelection could not open a socket for communication.
	Action	The network administrator should make sure the side A and B servers can communicate with each other.
1530235	Message	MasterSelection has been started.
	Severity	Informational
	Type	Clear
	Description	MasterSelection IP addresses have been checked, a socket opened, and threads started.
	Action	No action is required.
1530025	Message	An attempt was made to remove an agent from a skill group and either the agent or the skill group does not exist.
	Severity	Error
	Type	Raise
	Description	AAS attempted to remove an agent from a skill group and either the agent or the skill group does not exist.
	Action	Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).
1530026	Message	An attempt was made to remove an agent from a skill group where no such assignment exists.
	Severity	Error
	Type	Raise
	Description	An attempt was made to remove an agent from a skill group where no such assignment exists.
	Action	Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).

Message ID (hex)	Property	Value
1530003	Message	The maximum SEI event queue size was exceeded.
	Severity	Error
	Type	Raise
	Description	The maximum SEI event queue size was exceeded.
	Action	Change the configuration in the registry (see Troubleshooting Guide) to allow for a greater queue size.
1530040	Message	AAS failed to establish a connection to SEI.
	Severity	Error
	Type	Raise
	Description	AAS failed to establish a connection to SEI.
	Action	No action is required.
1530027	Message	A request was made to add an agent in a bulk operation where no corresponding person exists.
	Severity	Error
	Type	Raise
	Description	A request was made to add an agent in a bulk operation where no corresponding person exists.
	Action	No action is required.
1530041	Message	The maximum allowable event queue size has been exceeded.
	Severity	Error
	Type	Raise
	Description	The maximum event queue size has been exceeded even though the ICM/AW appears to be functioning as usual. Some causes are a slow network, a slow ICM/AW, or a slow database.
	Action	The problem may be fixed by increasing the value in the AASSEIMaxEventQueueSize registry (see Troubleshooting Guide) setting.

Message ID (hex)	Property	Value
1530035	Message	All attempts to connect to Symposium have failed.
	Severity	Error
	Type	Raise
	Description	All attempts to connect to Symposium have failed.
	Action	Ensure that all the Symposium services are started and running. Check that the Symposium configuration/connection information is correct.
1530036	Message	Error performing post resync processing.
	Severity	Error
	Type	Raise
	Description	There was an error while performing post-resync processing. The error occurred during ICM/AW processing while trying to cache data from the ICM database.
	Action	Check for a broken connection to the ICM or other errors in the log for problems accessing the database.
1530037	Message	An event was discarded.
	Severity	Error
	Type	Raise
	Description	An event was discarded due to a data access exception received from ICM/AW (ConAPI).
	Action	No action is required.
1530057	Message	Due to the max event queue size being exceeded, a resync of Symposium events is being requested.
	Severity	Error
	Type	Raise
	Description	A Symposium resync is being requested because the maximum event queue size has been exceeded.
	Action	This is due to a configuration error in the registry. Check the registry (see Troubleshooting Guide) and make sure it is correct.

Message ID (hex)	Property	Value
1530038	Message	Registration with SEI server failed.
	Severity	Error
	Type	Raise
	Description	The registration with SEI server failed.
	Action	Ensure the SEI configuration in the registry (see Troubleshooting Guide) is correct.
1530039	Message	Request for initial SEI events failed.
	Severity	Error
	Type	Raise
	Description	The request for initial SEI events failed.
	Action	Make sure the Symposium services are started and functioning properly.