Serviceability Best Practices Guide for Cisco ICM/Unified Contact Center Enterprise, Release 10.5(1)

First Published: 2014-06-18

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 NONINFRINGEMENT 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.

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: www.cisco.com/go/trademarks. 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)

© 2003–2014 Cisco Systems, Inc. All rights reserved.
CONTENTS

PREFACE

Preface xiii
Change History xiii
About This Guide xiii
Audience xiii
Organization xiv
Related Documents xv
Obtaining Documentation and Submitting a Service Request xv
Field Alerts and Field Notices xv
Documentation Feedback xv
Conventions xv

CHAPTER 1

Product Architecture 1
Cisco Unified Contact Center 1
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
Computer Telephony Integration Option 7
Cisco Agent Desktop 7
Configuration System 9
   Administration & Data Server 9
   Configuration Updates 10
Reporting System 10
   Historical Data Server 10
   Unified Intelligence Center 11
      Unified Intelligence Center Standard Deployment Model 12
      Unified Intelligence Center Scaled Deployment Model 12
   Unified Contact Center Management Portal 13
Outbound Option 16

CHAPTER 2
Monitoring SNMP Health 19
SNMP Overview 19
   Faults 19
   Instrumentation 21
Base-Level SNMP MIB Support 21
SNMP Master Agent 21
Base Level SNMP Subagents 21
   Platform MIB Support 22
   Host Resources MIB Subagent 22
   Cisco Discovery Protocol (CDP) MIB Subagent 23
   MIB2 23
   SYSAPPL MIB Subagent 23
CISCO-CONTACT-CENTER-APPS-MIB 24
   CISCO-CONTACT-CENTER-APPS-MIB Overview 24
   CISCO-CONTACT-CENTER-APPS-MIB Structure 24
   Mapping CCCA-MIB to Standard Host MIBs 26
   CISCO-CONTACT-CENTER-APPS-MIB Objects 28
      CCCA MIB Base Objects 29
      CCCA MIB Instance Table Objects 29
      CCCA MIB Component Table Objects 30
      CCCA MIB Component Element Table Objects 31
      CCCA MIB Router Table Objects 32
CHAPTER 5  Services and Processes  67
  Services  67
  Using the Local Desktop  78
  ICM Service Control and Windows Task Manager  78
  Using the Local Registry  78
  Using the Remote SNMP Management Station  79

CHAPTER 6  Contact Center Trace Levels  81
  Trace Levels  81
    Trace–All Nodes  82
    Trace–Administration and Data Server (Previously Known as the Distributor Administrator Workstation)  82
    Trace–Router  83
    Trace–Logger  83
    Trace–Peripheral Gateway  84
    Trace–Web Setup  86
    Trace–Diagnostic Framework  86
  EMS Log Compression  87
    Dumplog  87
    EMS File Compression Control  87
    Other Registry Keys  87
  Set Router Tracing  87
  How to Set OPC Tracing  89
    General Diagnostics  89
    Diagnosing Network Transfer Issues  89
    Diagnosing Multimedia Issues  90
    Diagnosing VRU PG Issues  90
    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  91
    How to Set JTAPI Gateway Default Tracing  91
  How to Set CTI Server Tracing  91
Setting CTI Server Default Tracing  
Setting CTI OS Tracing  
Setting VRU PIM Tracing  
Setting VRU PIM Default Tracing  
Setting Outbound Option Tracing  
How to Reset CampaignManager Tracing  
How to Reset baImport Tracing  
How to Reset Dialer Tracing  
Trace File Retention Settings  
Router Full Dump Enabled by Default

CHAPTER 7

Performance Counters  
Import Unified CCE Data Collector Set Template  
Platform Health Monitoring Counters  
Platform Diagnostic Counters – Automatic Collection  
Platform Diagnostic Counters  
All Components  
Logger/Administration & Data Server/HDS  
SQL Server  
Component-Specific Counters  
Router  
Logger  
Administration & Data Server  
PG – OPC  
PG – Communications Manager (EA) PIM  
PG – VRU PIM  
CTI Server  
CTI OS Server  
Outbound Option Campaign Manager  
Outbound Option Import  
Outbound Option Dialer  
Message Delivery Service  
QoS  
QoS Marking for Live Data (PCCE Deployments Only)
### Chapter 8: Capacity Planning

- **Capacity Planning** 137
  - Capacity Planning Process 137
  - Capacity Planning – Getting Started 138
  - Finding the Busy Hour 138
- **Collected Data Categorization** 139
  - Current Deployment Design 139
  - Configuration Information 140
  - Traffic Load 141
  - Migration Requirements 141
  - Platform Performance 142
- **Capacity Utilization** 142
  - CPU Utilization Calculations 143
  - Memory Utilization Calculations 143
  - Disk Utilization Calculations 144
  - NIC Utilization Calculations 144
  - Maximum Utilization Calculations 144
  - Relating Traffic Load to Resources 144

### Chapter 9: Diagnostic Tools

- **Diagnostic Framework** 147
  - Overview 147
  - Installation and Configuration 147
    - Service Registration and Dependencies 148
    - Configure Service Port 148
    - Installing or Updating Third-Party Certificate 149
    - Diagnostic Framework Log Files and Logging Level 149
    - Diagnostic Framework Service Resources Requirements 150
  - Security 151
    - Authentication, Authorization, and Auditing 151
    - Encryption 153
    - Certificate Management 153
  - Usage 156
Accessing the Diagnostic Framework Through the Analysis Manager 156
Accessing the Diagnostic Framework Through the Unified System CLI 156
Accessing the Diagnostic Framework Through the Built-In User Interface (Portico) 181
Accessing Diagnostic Framework Commands Through a Browser 183

CLI Configuration 183

Deployment Option 1: CVP OAMP 184
  Configure System CLI with CVP OAMP 184
  Modify or Add User to CVP OAMP for System CLI 185
  Install CVP Remote Operations 186
  Add Remote Operations Machines to CVP Operations Console 187
  Confirm Windows Environment Variables Set Correctly for CVP Web Services 187
  Use Unified System CLI with CVP OAMP 188

Deployment Option 2: Devices.csv 188
  Create Devices.csv from Sample File 189
  Add Connection Information to Devices.csv File 189
  Designate Users for Diagnostic Framework 190
  Use Unified System CLI with Devices.csv 191
  Running the System CLI from Multiple Machines with Devices.csv 192

Diagnostic Framework API 192
  GetTraceLevel 192
  SetTraceLevel 193
  ListTraceComponents 193
  ListTraceFiles 195
  DownloadTraceFile 195
  ListLogComponents 196
  ListLogFile 197
  DownloadLogFile 197
  ListAppServers 198
  ListConfigurationCategories 198
  GetConfigurationCategory 199
  GetProductVersion 199
  GetProductLicense 199
  GetPlatformInformation 200
  GetNetStat 201
Contents

Administrator Workstation Events  283
Outbound Option Events  283
ICM Network Interface Controller (NIC) Events  294
ICM Hosted Events  349
Symposium/AAS Events  352
Live Data Events (Packaged CCE only)  362
Preface

- Change History, on page xiii
- About This Guide, on page xiii
- Audience, on page xiii
- Organization, on page xiv
- Related Documents, on page xv
- Obtaining Documentation and Submitting a Service Request, on page xv
- Field Alerts and Field Notices, on page xv
- Documentation Feedback, on page xv
- Conventions, on page xv

Change History

This table lists changes made to this guide. The newest changes are at the top of the table.

<table>
<thead>
<tr>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Various changes throughout the document to reflect the current release.</td>
<td>Initial release of document for 10.5(1).</td>
</tr>
</tbody>
</table>

About This Guide

This guide describes Cisco Unified Intelligent Contact Management Enterprise (ICM)/Unified Contact Center Enterprise (CCE) from a management perspective, and describes the capabilities of the management interfaces and features. This guide enables the reader to formulate a management and monitoring strategy or easily integrate the management of Unified ICM/Unified CCE into an existing network management infrastructure.

The focus of this document is Unified CCE. Most of the content and serviceability features are supported by Unified ICM as well. If content is specific to one product or the other, the product is noted.

Audience

This guide is intended for system administrators who monitor and manage Unified CCE/Unified CCH and Unified ICME/Unified ICMH.
## Organization

<table>
<thead>
<tr>
<th>Section</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1: Product Architecture</td>
<td>This chapter provides an overview of the Cisco Unified Contact Center Enterprise architecture, and describes the configuration system and reporting system.</td>
</tr>
<tr>
<td>Chapter 2: Monitoring SNMP Health</td>
<td>This chapter describes SNMP Health Monitoring, including base-level SNMP MIB support and the CISCO-CONTACT-CENTER-APPS-MIB. This chapter also describes how to configure SNMP agents.</td>
</tr>
<tr>
<td>Chapter 3: Understanding Unified ICM/Unified CCE SNMP Notifications</td>
<td>This chapter provides information about Unified ICM/Unified CCE SNMP notification types, dual and single state objects, and CSFS heartbeat notification. This chapter also describes how to correlate and organize notifications.</td>
</tr>
<tr>
<td>Chapter 4: The syslog Messaging Interface</td>
<td>This chapter provides information about syslog messaging, including a description of the Cisco Log Message format and how to configure syslog destinations.</td>
</tr>
<tr>
<td>Chapter 5: Unified ICM/Unified CCE Services and Processes</td>
<td>This chapter describes the services and processes running on a particular server and how to obtain information about those services and processes using the local desktop, ICM Service Control and Windows Tasks Manager, local registry, and Remove SNMP Management Station.</td>
</tr>
<tr>
<td>Chapter 6: Unified ICM/Unified CCE Trace Levels</td>
<td>This chapter describes trace levels for each solution component and how to set tracing for those components. It also provides information about EMS log compression.</td>
</tr>
<tr>
<td>Chapter 7: Performance Counters</td>
<td>This chapter describes the performance counters that determine the health of the system, including health monitoring counters, diagnostic counters, component-specific counters, and (for Cisco Packaged Contact Center Enterprise deployments only) Live Data performance counters.</td>
</tr>
<tr>
<td>Chapter 8: Capacity Planning</td>
<td>This chapter describes how to determine the current solution capacity, estimate growth potential, and answer &quot;what if&quot; scenarios.</td>
</tr>
<tr>
<td>Chapter 9: Unified ICM/Unified CCE Diagnostic Tools</td>
<td>This chapter provides information about the configuration, security, and usage of the Diagnostic Framework.</td>
</tr>
<tr>
<td>Appendix A: Cisco Contact Center Applications MIB Results Example</td>
<td>This appendix provides an example of the data returned by the Cisco Contact Center Applications MIB SNMP agent.</td>
</tr>
<tr>
<td>Appendix B: Unified ICM/Unified CCE SNMP Notifications</td>
<td>This appendix describes each SNMP notification for Unified ICM/Unified CCE, and includes the Message ID, message text, severity, type, and action for each message.</td>
</tr>
</tbody>
</table>
Related Documents

<table>
<thead>
<tr>
<th>Document or resource</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation Guide</td>
<td>unified-contact-center-enterprise/</td>
</tr>
<tr>
<td></td>
<td>products-documentation-roadmaps-list.html</td>
</tr>
<tr>
<td>Center Enterprise documentation</td>
<td>unified-contact-center-enterprise/</td>
</tr>
<tr>
<td></td>
<td>tsd-products-support-series-home.html</td>
</tr>
<tr>
<td></td>
<td>unified-contact-center-enterprise/</td>
</tr>
<tr>
<td></td>
<td>products-device-support-tables-list.html</td>
</tr>
</tbody>
</table>

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Field Alerts and Field Notices

Cisco can modify its products or determine key processes to be important. These changes are announced through use of the Cisco Field Alerts and Cisco Field Notices. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

Sign in www.cisco.com and then access the tool at https://www.cisco.com/cisco/support/notifications.html.

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:
<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **boldface** font | Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example:  
  • Choose **Edit** > **Find**.  
  • Click **Finish**. |
| *italic* font | Italic font is used to indicate the following:  
  • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills.  
  • A syntax value that the user must replace. Example: IF *(condition, true-value, false-value)*  
  • A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*. |
| **window** font | Window font, such as Courier, is used for the following:  
  • Text as it appears in code or that the window displays. Example:  
    `<html><title>Cisco Systems, Inc. </title></html>` |
| `< >`         | Angle brackets are used to indicate the following:  
  • 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. |
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 9
- Reporting System, on page 10
- Outbound Option, on page 16

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*

![Unified CCE Architecture Diagram]

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 normally.
**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 executes 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**

Unified ICME/Unified ICMH only

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.
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 master 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 master 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.
Coresident with the PG is the CTI Gateway (CG - CTI Server component) and the Cisco Computer Telephony Integration Option (CTI OS).

**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/Unified CCH 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

Unified ICME/Unified ICMH only

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/Unified CCH 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:

- CTI OS – the client of choice for agent and supervisor desktops, and CRM integration.
- 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 ACM.

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

Computer Telephony Integration Option

The Computer Telephony Integration Option (CTI OS) is the connection from the PG to desktop clients and is also used for CRM integration. CTI OS completes the abstraction of peripheral type. The set of messages and commands are the same no matter what type of peripheral you connect the PG to.

CTI OS is also used as the per-agent connection to the Cisco Agent Desktop. CTI OS can connect to both Side A and Side B CTI Servers to provide a reliable connection.

Cisco Agent Desktop

The Cisco Agent Desktop (CAD) base services consist of a set of services that run as Windows Server services. The base services include:
• Chat Service
• Directory Services
• Service
• Browser and IP Phone Agent Service
• LDAP Monitor Service
• Licensing and Resource Manager Service
• Recording and Statistics Service
• Sync Service
• Tomcat Web Service

The Enterprise Service and BIPPA Service interact with the CTI service, typically running on a PG. You can place additional services on the same or separate computer as the base services. These additional services include:

• Voice over IP Monitor Service
• Recording & Playback Service

A set of the base services plus the additional services is a logical contact center, or LCC. The maximum number of agents that can be supported by a single LCC is 2,000 (approximately 15,000 Busy Hour Call Completion [BHCC] with a call volume of 20 calls per agent per hour).

The Cisco Agent Desktop services typically reside coresident on the same server with PG and CTIOS services.

Service Names/Executables

To check if a service is running, use the following table to match the name shown in the Services window (accessed through the Windows control panel) with a particular executable.

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Executable Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Browser and IP Phone Agent Service</td>
<td>IPPASvr.exe</td>
</tr>
<tr>
<td>Cisco Chat Service</td>
<td>FCCServer.exe</td>
</tr>
<tr>
<td>Cisco Service</td>
<td>CTI Storage Server.exe</td>
</tr>
<tr>
<td>Cisco LDAP Monitor Service</td>
<td>LDAPmonSvr.exe</td>
</tr>
<tr>
<td>Cisco Licensing and Resource Manager Service</td>
<td>LRMServer.exe</td>
</tr>
<tr>
<td>Cisco Recording &amp; Playback Service</td>
<td>RPServer.exe</td>
</tr>
<tr>
<td>Cisco Recording and Statistics Service</td>
<td>FCRasSvr.exe</td>
</tr>
<tr>
<td>Cisco Sync Service</td>
<td>DirAccessSynSvr.exe</td>
</tr>
<tr>
<td>Cisco VoIP Monitor Service</td>
<td>FCVoIPMonSvr.exe</td>
</tr>
<tr>
<td>Directory Replication Service</td>
<td>slurpd.exe</td>
</tr>
<tr>
<td>Directory Services</td>
<td>slapd.exe</td>
</tr>
<tr>
<td>Tomcat Service</td>
<td>tomcat5.exe</td>
</tr>
</tbody>
</table>

**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 executed (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.
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, Unified ICMH, Unified CCE and Unified CCH.

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
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

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

*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 and Unified CCH 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 that 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 normally 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, for example agents or skill groups, the Unified CCMP can optionally record the events logged by the equipment, such as call records 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 you access by a web browser (Microsoft Internet Explorer). 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.
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 Dialers make the calls, performing the two tasks of agent reservation and dialing. The IP Dialer uses the MR PG to reserve an agent to handle the call and it talks to Unified Communications Manager directly using Skinny Call Control Protocol (SCCP) (Communications Manager phone protocol) to dial. After everything is connected, it uses Unified Communications Manager to connect the call.

The Outbound Option Dialer maximizes the resources in a contact center by dialing several customers per agent. This component resides on the PG server.
Outbound Option deployments can use the Session Initiation Protocol (SIP) Dialer alongside the SCCP Dialer. In an Outbound Option deployment that uses the SIP Dialer, functions such as dialing, call control, and Voice Gateway, and not the Unified CM, handles the Call Progress Analysis for Outbound campaigns. This increases the number of Outbound agents that a deployment can service on a PG, and 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*
Monitoring SNMP Health

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):

```plaintext
cccaIcmEvent NOTIFICATION-TYPE
OBJECTS {
    cccaEventComponentId,
    cccaEventState,
    cccaEventMessageId,
    cccaEventOriginatingNode,
    cccaEventOriginatingNodeType,
    cccaEventOriginatingProcessName,
    cccaEventOriginatingSide,
}```
A detailed description of each object in the notification type is found in `cccamEvent`, 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 execute 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 Master Agent**

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

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

The master 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 master 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 for cccaComponentElmtRunID.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
```
The implementation approach for standardized MIBs, such as the Host Resources MIB, can vary from vendor to vendor, subject to interpretation. For example, the hrSWRunStatus object 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 the object value is polled. Later changes to the SNMP subagent are aligned with this assumption: any process loaded is considered running even if it is not allocated CPU cycles.

**Cisco Discovery Protocol (CDP) MIB Subagent**

The CDP is a Cisco-proprietary network protocol used (for our purposes) to broadcast device discovery information to routers or switches in the network. Cisco Unified Operations Manager can use this device discovery data to build a network topology and to identify devices within that topology. This means that a network administrator can click the device icon for a product node and quickly identify it.

The CDP driver may cause low-level system halts (blue screens for example) if installed on servers with an unsupported NIC chipset. This is the reason that the CDP driver and subagent is optionally installed for Unified ICM/Unified CCE.

**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 executing 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 (CTIOS)
- 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 CTIOS 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: CCCA 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 cccaComponentTable. 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 executing, 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 CCCA-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.
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/Unified CCH 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.
Active (5)

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

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 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 Unified ICMH or Unified CCH 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 normal 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.
**ccaRouterPublicNonHighAddr**

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.

**ccaRouterPrivateHighAddr**

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.

**ccaRouterPrivateNonHighAddr**

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.

**ccaNicIndex**

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.

**ccaNicType**

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

**ccaNicStatus**

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.

**cccLoggerSide**

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'.

**cccLoggerType**

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.

**cccLoggerRouterSideAName**

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.

**cccLoggerRouterSideBName**

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.

**cccLoggerDuplexPairName**

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.

**cccLoggerHDSReplication**

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.

**cccLoggerAvgDBWriteTime**

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.

**cccaPdDuplexPairName**

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.
ccccPimPeripheralName

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

ccccPimPeripheralType

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.

ccccPimStatus

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

ccccPimPeripheralHostName

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.

ccccCgNumber

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.

ccccCgSide

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’.

ccccCgPgSideAName

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.

ccccCgPgSideBName

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.
**cccA CgDuplexPairName**

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.

**cccA CgOpenSessions**

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 normally.

**cccA CgOtherSessions**

The CG other sessions objects indicates the total number of sessions (connections) between the CTI Gateway and CTI clients that are not normal, 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 normal operation. A steadily increasing value indicates a problem that should be investigated.

**cccA CgID**

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.

**cccA CtiOsServerName**

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

**cccA CtiOsPeripheralName**

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.

**cccA CtiOsPeripheralType**

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.

**cccA CtiOsCgSideAName**

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.
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.

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.

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.

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.

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.

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.

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 Side A 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 (side A), 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 Side A 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. By default, the campaign manager deliberately restarts when this value exceeds 10,000 messages in queue as a self-defense mechanism; the administrator must then investigate the reason for this performance bottleneck.

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.

**cccDialerCampaignMgrName**

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.

**cccDialerCampaignMgrStatus**

The Dialer campaign manager status indicates the current connection status between this Dialer and the Outbound Option Campaign Manager component, which is co-resident with the Logger (side A).

**cccDialerCtiServerAName**

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 executes call control after an available agent is selected.

**cccDialerCtiServerBName**

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 executes call control after an available agent is selected.

**cccDialerCtiServerStatus**

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

**cccDialerMediaRouterStatus**

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.

**cccDialerQueueDepth**

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. By default, the Dialer process deliberately restarts when this value exceeds 10,000 messages.

```
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
```

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 normal 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 the course of normal 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.

---

**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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Start menu select <strong>Run</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Start box type in <code>mmc /32</code> and press <strong>Enter</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the Console, select <strong>File &gt; Add/Remove Snap-in</strong>. A new window appears.</td>
</tr>
<tr>
<td>Step 4</td>
<td>From the <strong>Standalone</strong> tab, verify <strong>Console Root</strong> is selected in the <strong>Snap-ins added to:</strong> field and click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Add Snap-in window scroll down and select <strong>Cisco SNMP Agent Management</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Add Snap-in window click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Step 7</td>
<td>In the Add Snap-in window click <strong>Close</strong>.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Click <strong>OK</strong> in the Add/Remove Snap-in window.</td>
</tr>
</tbody>
</table>

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.
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.
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.
Configure User Names for SNMP v3

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](image)

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.
   a) choose an authentication protocol
   b) 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.
   a) Choose an encryption type.
   b) 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.
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

- SNMP System Information:
  - System Name: Some CGRect Cisco.com
  - System Location: 3rd Floor Lab
  - System Contact: Lab Administrator
  - System Description: Cisco Contact Center Application Server
  - SNMP Port Number: 161
  - Enable Authentication Traps?

- Agent Performance
  - Execution Priority:
    - Normal
    - Low
  - Maximum Limits:
    - Concurrent Requests: 5
    - Subagent Wait Time: 25
    - Subagents: 25
  - Agent Log Quantity:
    - Verbose
    - Normal
    - terse

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.

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>The fully qualified domain name of the system. If empty, this automatically fills.</td>
</tr>
<tr>
<td>System Location</td>
<td>The physical location of the server itself, for example, Building 5, Floor 3, Room 310.</td>
</tr>
<tr>
<td>System Contact</td>
<td>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.</td>
</tr>
<tr>
<td>System Description</td>
<td>A brief description of this server, to include the primary application running on the server.</td>
</tr>
<tr>
<td>Number</td>
<td>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.</td>
</tr>
<tr>
<td>Enable Authentication Traps</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 master agent waits for a subagent response.

**Subagents**

The maximum allowable subagents that the master 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:
Configure SNMP Trap Destinations

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**.
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

cccaIcmEvent

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

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

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cccaEventComponentId</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Object Name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| cccaEventState                | 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:  
  'clear' (0): The clear state indicates that the condition that generated a previous raise notification is resolved.  
  '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.  
  '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.  
  '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            | 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. |
| cccaEventOriginatingNode      | 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>
<table>
<thead>
<tr>
<th>Object Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cccaEventOriginatingNodeType</td>
<td>The type of enterprise contact center application functional component or subcomponent that generated this notification. The node types are: 'unknown' (0): The notification originates from an unknown source. 'router' (1): The notification was generated by the Router functional component. 'pg' (2): The notification was generated by the peripheral gateway functional component. 'nic' (3): The notification was generated by the network interface controller functional component. 'aw' (4): The notification was generated by the administrator workstation functional component. 'logger' (5): The notification was generated by the Logger functional component. '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). 'cg' (7): The notification was generated by the CTI gateway functional component. '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.</td>
</tr>
<tr>
<td>cccaEventOriginatingProcessName</td>
<td>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.</td>
</tr>
<tr>
<td>cccaEventOriginatingSide</td>
<td>The enterprise contact center application functional component fault tolerant side (either 'A' or 'B') that generated this notification.</td>
</tr>
<tr>
<td>cccaEventDmpId</td>
<td>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.</td>
</tr>
</tbody>
</table>
**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 normally.

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.

```plaintext
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
```

---

Serviceability Best Practices Guide for Cisco ICM/Unified Contact Center Enterprise, Release 10.5(1)
Understanding SNMP Notifications

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 4: Example: Raise Notification

<table>
<thead>
<tr>
<th>Field</th>
<th>Value / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTIFICATION</td>
<td>1028105</td>
</tr>
<tr>
<td>cccaEventMessageId</td>
<td>2701295877 (0xA1028105)</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>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.</td>
</tr>
<tr>
<td>cccaEventState</td>
<td>Raise</td>
</tr>
<tr>
<td>SUBSTITUTION STRING</td>
<td>The operator/administrator has shut down the ICM software on %1.</td>
</tr>
<tr>
<td>ACTION</td>
<td>Contact the operator/administrator to determine the reason for the shutdown.</td>
</tr>
<tr>
<td>cccaEventComponentId</td>
<td>{cccaEventOriginatingNode %1}</td>
</tr>
<tr>
<td>CorrelationId</td>
<td>{ CLASS_NM_INITIALIZING cccaEventOriginatingNode %1 }</td>
</tr>
</tbody>
</table>

Table 5: Example: Clear Notification

<table>
<thead>
<tr>
<th>Field</th>
<th>Value / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTIFICATION</td>
<td>1028103</td>
</tr>
<tr>
<td>cccaEventMessageId</td>
<td>1627554051 (0x61028103)</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>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.</td>
</tr>
<tr>
<td>cccaEventState</td>
<td>Clear</td>
</tr>
<tr>
<td>SUBSTITUTION STRING</td>
<td>%1 Node Manager started. Last shutdown was by operator request.</td>
</tr>
<tr>
<td>ACTION</td>
<td>No action is required.</td>
</tr>
<tr>
<td>cccaEventComponentId</td>
<td>{ cccaEventOriginatingNode %1 }</td>
</tr>
</tbody>
</table>
**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.
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 6: Example "Single-State Raise" Notification**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTIFICATION</td>
<td>105023C</td>
</tr>
<tr>
<td>cccaEventMessageId</td>
<td>3775201852 (0xE105023C)</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>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.</td>
</tr>
<tr>
<td>cccaEventState</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td>SUBSTITUTION STRING</td>
<td>The Router has detected that it is no longer synchronized with its partner.</td>
</tr>
<tr>
<td>ACTION</td>
<td>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&lt;instance&gt;\ra directory of Router A and in the icm&lt;instance&gt;\rb directory of Router B. Contact the.</td>
</tr>
<tr>
<td>cccaEventComponentId</td>
<td>{ cccaEventOriginatingNode cccaEventOriginatingProcessName cccaEventOriginatingSide }</td>
</tr>
<tr>
<td>CorrelationId</td>
<td>{ CLASS_RTR_SYNC_CHECK cccaEventOriginatingNode cccaEventOriginatingProcessName cccaEventOriginatingSide }</td>
</tr>
</tbody>
</table>
## 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.

```plaintext
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:

```
CCBU-CSA-RGR1A

acme

routerA
```

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 7: CSFS Heartbeat Notification

<table>
<thead>
<tr>
<th>Field</th>
<th>Value / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTIFICATION</td>
<td>12A0003</td>
</tr>
<tr>
<td>cccaEventMessageId</td>
<td>1630142467 (0x612A0003)</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>Periodic message to indicate MDS is in service and that the event stream is active.</td>
</tr>
<tr>
<td>cccaEventState</td>
<td></td>
</tr>
<tr>
<td>SUBSTITUTION STRING</td>
<td>HeartBeat Event for %1</td>
</tr>
</tbody>
</table>
### 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:

```plaintext
HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\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 normally 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.
CSFS Heartbeat Notification
Syslog Messaging 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: HOURS: 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRI</td>
<td>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.</td>
</tr>
<tr>
<td>SEQNUM</td>
<td>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.</td>
</tr>
<tr>
<td>HOST</td>
<td>Fully qualified domain name (FQDN), hostname, or IP address of the originating system.</td>
</tr>
<tr>
<td>MONTH</td>
<td>Current month represented in MMM format (for example, “Jan” for January)</td>
</tr>
<tr>
<td>DAY</td>
<td>Current day represented in DD format. Range is 01 to 31.</td>
</tr>
<tr>
<td>YEAR</td>
<td>Current year represented in YYYY format.</td>
</tr>
<tr>
<td>HOUR</td>
<td>Hour of the timestamp as two digits in 24-hour format; range is 00 to 23.</td>
</tr>
<tr>
<td>MINUTE</td>
<td>Minute of the timestamp as two digits; range is 00 to 59.</td>
</tr>
</tbody>
</table>
### 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*

The steps run the CW2KFEED process when the logger is started.

**Procedure**

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

**Step 2** 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 3** Right-click the white space in right pane and select **Properties**. A dialog box appears:
Configure Syslog Destinations

Figure 21: Syslog Destinations Properties Dialog Box

Step 4  From the **ICM/IPCC Instances** list box, select one Unified ICM/Unified CCE instance. The **Instance** field displays the selected instance.

Step 5  Check **Enable Feed?** check box.

Step 6  In the **Collector Address** field, enter the IP address or Host Name.

Step 7  *(Optional)* In the **Port** field, enter the collector port number on which syslog collector is listening.

  **Note**  The default port is 514.

Step 8  Click **Insert** to add the IP address to the list.

  **Note**  You can add up to five IP addresses.

Step 9  *(Optional)* To remove an existing IP address, select the IP address in the **Collector Address List** area, and click **Remove**.

Step 10  *(Optional)* Check **Disable Ping Tests?** check box.

Step 11  Click **Save**.

Step 12  Click **OK**.
# Services and Processes

- Services, on page 67
- Using the Local Desktop, on page 78
- ICM Service Control and Windows Task Manager, on page 78
- Using the Local Registry, on page 78
- Using the Remote SNMP Management Station, on page 79

## 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 normal 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>
<thead>
<tr>
<th>Component</th>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>* router.exe</td>
<td>[Critical] This is the primary Router process.</td>
</tr>
<tr>
<td></td>
<td>* rtsvr.exe</td>
<td>[Critical] Provides real-time data feed from the Router to the Administration &amp; Data Server.</td>
</tr>
<tr>
<td></td>
<td>* mdsproc.exe</td>
<td>[Critical] Message Delivery Service</td>
</tr>
<tr>
<td></td>
<td>* ccagent.exe</td>
<td>[Critical] Router component that manages communication links between the Router and peripheral gateways.</td>
</tr>
<tr>
<td></td>
<td>* dbagent.exe</td>
<td>[Critical] Manages connections and transactions (configuration updates) from configuration tools.</td>
</tr>
<tr>
<td></td>
<td>* testsync.exe</td>
<td>[Non critical] Provides interface for component test tools.</td>
</tr>
<tr>
<td></td>
<td>* appgw.exe</td>
<td>[Optional/Critical] The process that provides an interface for the Router to communicate with external applications.</td>
</tr>
<tr>
<td></td>
<td>* dbworker.exe</td>
<td>[Optional/Critical] The process that provides the interface for the Router to query external databases.</td>
</tr>
<tr>
<td></td>
<td>* [NIC].exe</td>
<td>[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. The presence of a NIC process in a Unified CCE deployment is very rare. NIC process names: attnic.exe, caulnic.exe, netwrknic.exe, crspnic.exe, gktmpnic.exe, incrpnic.exe, mcnic.exe, gennnic.exe, nttnic.exe, ntlnic.exe, sprnic.exe, ss7innic.exe, stentonic.exe, timnic.exe, unisourcenic.exe</td>
</tr>
<tr>
<td>Component</td>
<td>Process</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logger</td>
<td>* configlogger.exe</td>
<td>[Critical] The process that manipulates configuration data.</td>
</tr>
<tr>
<td></td>
<td>* histlogger.exe</td>
<td>[Critical] The process that inserts historical data into TMP historical tables in the Logger database.</td>
</tr>
<tr>
<td></td>
<td>* recovery.exe</td>
<td>[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.</td>
</tr>
<tr>
<td></td>
<td>* replication.exe</td>
<td>[Critical] The process that replicates data from the Logger to the Historical Data Server on an Administration &amp; Data Server.</td>
</tr>
<tr>
<td></td>
<td>* csfs.exe</td>
<td>[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.</td>
</tr>
<tr>
<td></td>
<td>* cw2kfeed.exe</td>
<td>[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.</td>
</tr>
<tr>
<td></td>
<td>* campaignmanager.exe</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Process</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[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 in memory. The Campaign Manager also sends real time and historical data to the Router and distributes configuration information to Dialer and Import processes.</td>
</tr>
<tr>
<td></td>
<td>* baimport.exe</td>
<td>[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.</td>
</tr>
<tr>
<td></td>
<td>sqlservr.exe</td>
<td>[Critical] Microsoft SQL server process</td>
</tr>
<tr>
<td></td>
<td>sqlagent.exe</td>
<td>[Critical] Microsoft SQL server process</td>
</tr>
<tr>
<td>Component</td>
<td>Process</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PG</td>
<td>* opc.exe</td>
<td>[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.</td>
</tr>
<tr>
<td></td>
<td>* mdsproc.exe</td>
<td>[Critical] Message Delivery Service</td>
</tr>
<tr>
<td></td>
<td>* pgagent.exe</td>
<td>[Critical] MDS Peripheral Gateway component that manages the interface between the peripheral gateway and the central controller.</td>
</tr>
<tr>
<td></td>
<td>* testsync.exe</td>
<td>[Non critical] Provides interface for component test tools.</td>
</tr>
</tbody>
</table>
|                 | * 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.                                      |
<p>|                 | * 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 |                                                                                                                                             |</p>
<table>
<thead>
<tr>
<th>Component</th>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>[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.</td>
</tr>
<tr>
<td>* mrpim.exe</td>
<td></td>
<td>[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 Email Interaction Manager (EIM) and Web Interaction Manager (WIM). There may be multiple instances of this process running.</td>
</tr>
<tr>
<td>* msgis.exe</td>
<td></td>
<td>[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.</td>
</tr>
<tr>
<td>* ctiosservernode.exe</td>
<td></td>
<td>[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.</td>
</tr>
<tr>
<td>* jtapigw.exe</td>
<td></td>
<td>[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.</td>
</tr>
<tr>
<td>* ctisvr.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Process</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>[Critical] CTI Gateway (CTI Server) process that processes (GED-188) messages between CTI OS and OPC. Note: In legacy implementations, CTI Server manages connections to CTI desktops.</td>
<td></td>
</tr>
<tr>
<td>IPPASvr.exe</td>
<td>[Optional/Critical] Cisco Agent Desktop: Cisco Browser and IP Phone Agent Service</td>
<td></td>
</tr>
<tr>
<td>FCCServer.exe</td>
<td>[Optional] Cisco Agent Desktop: Cisco Chat Service</td>
<td></td>
</tr>
<tr>
<td>LDAPmonSvr.exe</td>
<td>[Optional/Critical] Cisco Agent Desktop: Cisco LDAP Monitor Service</td>
<td></td>
</tr>
<tr>
<td>LRMServer.exe</td>
<td>[Optional/Critical] Cisco Agent Desktop: Cisco Licensing and Resource Manager Service</td>
<td></td>
</tr>
<tr>
<td>RPServer.exe</td>
<td>[Optional/Critical] Cisco Agent Desktop: Cisco Recording &amp; Playback Service</td>
<td></td>
</tr>
<tr>
<td>FCRasSvr.exe</td>
<td>[Optional/Critical] Cisco Agent Desktop: Cisco Recording and Statistics Service</td>
<td></td>
</tr>
<tr>
<td>DirAccessSynSvr.exe</td>
<td>[Optional/Critical] Cisco Agent Desktop: Cisco Sync Service</td>
<td></td>
</tr>
<tr>
<td>FCVoIPMonSvr.exe</td>
<td>[Optional/Critical] Cisco Agent Desktop: Cisco VoIP Monitor Service</td>
<td></td>
</tr>
<tr>
<td>slapd.exe</td>
<td>[Optional/Critical] Cisco Agent Desktop: Directory Services</td>
<td></td>
</tr>
<tr>
<td>tomcat5.exe</td>
<td>[Optional/Critical] Cisco Agent Desktop: Tomcat Service</td>
<td></td>
</tr>
<tr>
<td><em>badialer_ip.exe</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Process</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Optional/Critical] Outbound Option: This is the Dialer process that implements a dialing algorithm and places calls to customers during an outbound campaign. The Dialer monitors skill groups for agent availability and reserves agents via the MR PG. The Dialer then informs the Campaign Manager of the result of each attempt to contact a customer.</td>
</tr>
<tr>
<td>Component</td>
<td>Process</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Administration &amp; Data Server (AW/HDS)</td>
<td>* configlogger.exe</td>
<td>[Critical] Processes inbound configuration data.</td>
</tr>
<tr>
<td></td>
<td>* updateaw.exe</td>
<td>[Critical] Updates the local configuration database with configuration data from the central controller.</td>
</tr>
<tr>
<td></td>
<td>* rtclient.exe</td>
<td>[Critical] Receives a real-time data feed (from a real-time distributor) and updates the local database.</td>
</tr>
<tr>
<td></td>
<td>* rtdist.exe</td>
<td>[Critical] Manages inbound real-time data from the real time server on the Router and distributes it to real-time clients.</td>
</tr>
<tr>
<td></td>
<td>* replication.exe</td>
<td>[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.</td>
</tr>
<tr>
<td></td>
<td>* cmsnode.exe</td>
<td>[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. 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.</td>
</tr>
<tr>
<td></td>
<td>* cms_jserver.exe</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Process</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Optional] Configuration Management System (CMS) Jaguar Server. This process works with cmsnode.exe for CMS to provide Java interfaces for ConAPI. 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.</td>
</tr>
<tr>
<td></td>
<td>* iseman.exe</td>
<td>[Optional] Internet Script Editor</td>
</tr>
<tr>
<td></td>
<td>sqlservr.exe</td>
<td>[Critical] Microsoft SQL server process</td>
</tr>
<tr>
<td></td>
<td>sqlagent.exe</td>
<td>[Optional] Microsoft SQL server process</td>
</tr>
<tr>
<td>Component</td>
<td>Process</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>All Nodes</td>
<td>nodeman.exe</td>
<td>[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.</td>
</tr>
<tr>
<td></td>
<td>nmm.exe</td>
<td>[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.</td>
</tr>
<tr>
<td></td>
<td>snmpdm.exe</td>
<td>[Important] SNMP master agent.</td>
</tr>
<tr>
<td></td>
<td>cccsnmpmgmt.exe</td>
<td>[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.</td>
</tr>
<tr>
<td></td>
<td>msnsaagt.exe</td>
<td>[Important] Microsoft native subagent adapter.</td>
</tr>
<tr>
<td></td>
<td>UcceSnmpHelperX86.exe</td>
<td>[Important] Used by hostagt.exe and ccaaagent.exe to get information about 32-bit processes that are currently running on the machine.</td>
</tr>
<tr>
<td></td>
<td>hostagt.exe</td>
<td>[Important] HOST-RESOURCES-MIB subagent.</td>
</tr>
<tr>
<td></td>
<td>sappagt.exe</td>
<td>[Important] SYSAPPL-MIB subagent.</td>
</tr>
<tr>
<td></td>
<td>ccaaagent.exe</td>
<td>[Important] CISCO-CONTACT-CENTER-APPS-MIB subagent.</td>
</tr>
</tbody>
</table>
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

On Windows 2008, 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 181.

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**

---

**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.
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)
```
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:

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

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

### Trace—All Nodes

You can set trace levels on these processes:

<table>
<thead>
<tr>
<th>Process</th>
<th>Level 0 (Default - Error)</th>
<th>Level 1 (Warning)</th>
<th>Level 2 (Informational)</th>
<th>Level 3 (Debug)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NM</td>
<td>0x00</td>
<td>0x0F</td>
<td>0x0F</td>
<td>0xFF</td>
</tr>
<tr>
<td>NMM</td>
<td>0x00</td>
<td>0x0F</td>
<td>0x0F</td>
<td>0xFF</td>
</tr>
</tbody>
</table>

The Diagnostic Framework does not support the Administrator Workstation.

### Trace—Administration and Data Server (Previously Known as the Distributor Administrator Workstation)

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

<table>
<thead>
<tr>
<th>Process</th>
<th>Level 0 (Default - Error)</th>
<th>Level 1 (Warning)</th>
<th>Level 2 (Informational)</th>
<th>Level 3 (Debug)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIGLOGGER</td>
<td>0x00</td>
<td>0x0F</td>
<td>0xFF</td>
<td>0xFFFF</td>
</tr>
<tr>
<td>CMSNODE</td>
<td>0x00</td>
<td>0x00</td>
<td>0x00</td>
<td>0xFFFFFEFFFF</td>
</tr>
<tr>
<td>CMS_JSERVER</td>
<td>0x00</td>
<td>0x00</td>
<td>0x00</td>
<td>0xFFFFFEFFFF</td>
</tr>
<tr>
<td>REPLICATION</td>
<td>0x00</td>
<td>0x0F</td>
<td>0xFF</td>
<td>0xFFF</td>
</tr>
<tr>
<td>RTCLIENT</td>
<td>0x00</td>
<td>0x0F</td>
<td>0xFF</td>
<td>0xFFF</td>
</tr>
<tr>
<td>RTDIST</td>
<td>0x00</td>
<td>0x0F</td>
<td>0xFF</td>
<td>0xFFF</td>
</tr>
</tbody>
</table>
The minimum and default trace level for the CMS, CMSJSer
er and ISE components is 2.

### Trace–Router

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

<table>
<thead>
<tr>
<th>Process</th>
<th>Level 0 (Default - Error)</th>
<th>Level 1 (Warning)</th>
<th>Level 2 (Informational)</th>
<th>Level 3 (Debug)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPGW</td>
<td>0x00</td>
<td>0x01</td>
<td>0x07</td>
<td>0x3F</td>
<td></td>
</tr>
<tr>
<td>CCAGENT</td>
<td>0x00</td>
<td>0x03</td>
<td>0x0F</td>
<td>0xFF</td>
<td></td>
</tr>
<tr>
<td>DBAGENT</td>
<td>0x00</td>
<td>0x01</td>
<td>0xFF</td>
<td>0xFF</td>
<td></td>
</tr>
<tr>
<td>DBWORKER</td>
<td>0x00</td>
<td>0x01</td>
<td>0xFF</td>
<td>0xFF</td>
<td></td>
</tr>
<tr>
<td>MDSPROC</td>
<td>0x00</td>
<td>0x07</td>
<td>0xFF</td>
<td>0xFF</td>
<td></td>
</tr>
<tr>
<td>ROUTER *</td>
<td>Turn off everything</td>
<td>Route Requests</td>
<td></td>
<td></td>
<td>Use RTRTRACE or RTRTEST</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Network VRU</td>
<td>- Call Queuing</td>
<td></td>
<td>Note: If you restart the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Trans Route</td>
<td>- Agent changes</td>
<td></td>
<td>Router process, the settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- VRU Bank</td>
<td>- Call Type Real Time</td>
<td></td>
<td>return to the default level.</td>
</tr>
<tr>
<td>RTSVR</td>
<td>0x00</td>
<td>0x0F</td>
<td>0xFF</td>
<td>0xFFF</td>
<td></td>
</tr>
</tbody>
</table>

### Trace–Logger

You can set trace levels on these processes for the Logger:
### Trace—Peripheral Gateway

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

<table>
<thead>
<tr>
<th>Process</th>
<th>Level 0 (Default - Error)</th>
<th>Level 1 (Warning)</th>
<th>Level 2 (Informational)</th>
<th>Level 3 (Debug)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAIMPORT</td>
<td>0xFF EMSUserData = 0xFFFF</td>
<td>0xFF EMSUserData = 0xFFFF</td>
<td>0xFF EMSUserData = 0xFFFF</td>
<td>0xFF EMSUserData = 0xFFFF</td>
</tr>
<tr>
<td>CAMPAIGN MANAGER</td>
<td>0xFF EMSUserData = 0xFFFF</td>
<td>0xFF EMSUserData = 0xFFFF</td>
<td>0xFF EMSUserData = 0xFFFF</td>
<td>0xFF EMSUserData = 0xFFFF</td>
</tr>
<tr>
<td>CONFIGLOGGER</td>
<td>0x00</td>
<td>0x0F</td>
<td>0xFF</td>
<td>0xFFF</td>
</tr>
<tr>
<td>CSFS</td>
<td>0x00</td>
<td>0x00</td>
<td>0x00</td>
<td>0xFF</td>
</tr>
<tr>
<td>CW2KFEED</td>
<td>0x00</td>
<td>0x00</td>
<td>0x00</td>
<td>0x07</td>
</tr>
<tr>
<td>DTP</td>
<td>0x00</td>
<td>0x04</td>
<td>0x06</td>
<td>0x0F</td>
</tr>
<tr>
<td>HISTLOGGER</td>
<td>0x00</td>
<td>0x0F</td>
<td>0xFFF</td>
<td>0xFFF</td>
</tr>
<tr>
<td>RECOVERY</td>
<td>0x00</td>
<td>0x0F</td>
<td>0xFFF</td>
<td>0xFFF</td>
</tr>
<tr>
<td>REPLICATION</td>
<td>0x00</td>
<td>0x0F</td>
<td>0xFFF</td>
<td>0xFFF</td>
</tr>
</tbody>
</table>

#### Trace—Peripheral Gateway

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

<table>
<thead>
<tr>
<th>Process</th>
<th>Level 0 (Default - Error)</th>
<th>Level 1 (Warning)</th>
<th>Level 2 (Informational)</th>
<th>Level 3 (Debug)</th>
</tr>
</thead>
<tbody>
<tr>
<td>JTAPIGW *</td>
<td>JT_JTAPI_EVENT_USED</td>
<td>JT_CONNECTION <em>CONF</em></td>
<td>JT_JTAPI* JT_HEX JT_ROUTE* JT_TERM* JT_LOW*</td>
<td>JT*</td>
</tr>
<tr>
<td>MDSPROC</td>
<td>0x00</td>
<td>0x07</td>
<td>0x0F</td>
<td>0xFF</td>
</tr>
<tr>
<td>MSGIS</td>
<td>0x00</td>
<td>0x00</td>
<td>0x00</td>
<td>0x3F</td>
</tr>
<tr>
<td>OPC **</td>
<td>Default, cstarcEMSTraceMask = 0x40</td>
<td>agent, inrcmsg, closedcalls, tspmsg, routing EMSTraceMask = 0x40 Note: Remove &quot;default&quot; tracing set in Default(0) level, but include cstarc.</td>
<td>Calls, NCT, simplified EMSTraceMask = 0x40 Note: Remove &quot;default&quot; tracing set in Default(0) level, but include Level 1.</td>
<td>Missingdata, halfhour EMSTraceMask = 0x40 Note: Remove &quot;default&quot; tracing set in Default(0) level, but include Level 2.</td>
</tr>
<tr>
<td>Process</td>
<td>Level 0 (Default - Error)</td>
<td>Level 1 (Warning)</td>
<td>Level 2 (Informational)</td>
<td>Level 3 (Debug)</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------</td>
<td>-------------------</td>
<td>-------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>PGAGENT</td>
<td>0x00</td>
<td>0x03</td>
<td>0x0F</td>
<td>0xFF</td>
</tr>
<tr>
<td>EAGTPIM</td>
<td>tp* precall <em>event csta</em></td>
<td>periph* jtapi_dialed*</td>
<td>autoconfig* teld*</td>
<td>lock* universal* service* threadid jtapi*</td>
</tr>
<tr>
<td>VRUPIM</td>
<td>EMSTraceMask= 0x0</td>
<td>EMSUserData= 0x71f7e0</td>
<td>EMSTraceMask= 0x0</td>
<td>EMSTraceMask= 0x0</td>
</tr>
<tr>
<td>ACMIPIM</td>
<td>EMSUserData = (hex) 01, 7f, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 3f, ff, ff, ff, ff, ff, ff, f0, fa</td>
<td>EMSUserData = (hex) f5, 7f, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 3f, ff, ff, ff, ff, ff, ff, f0, fa</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MRIPIM</td>
<td>Procmon:</td>
<td>EMSUserData = 0x40</td>
<td>EMSUserData = 0x58</td>
<td>EMSUserData = 0x5F</td>
</tr>
<tr>
<td>Avaya Aura PIM</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Tp* csta*, call*, csta*</td>
</tr>
<tr>
<td>AAS</td>
<td>Default</td>
<td>EMS_TRACE_GENERAL</td>
<td>EMS_TRACE_CONAPI</td>
<td>EMS_TRACE_AASDRIVER</td>
</tr>
<tr>
<td>Aspect PIM</td>
<td>Default</td>
<td>Default</td>
<td>Default</td>
<td>Tp* csta*, call*, csta*, app*, pim*, rtb*</td>
</tr>
</tbody>
</table>

Serviceability Best Practices Guide for Cisco ICM/Unified Contact Center Enterprise, Release 10.5(1)
### Trace—Web Setup

You can set trace levels on the Web Setup process.

<table>
<thead>
<tr>
<th>Process</th>
<th>Level 0 (Default - Error)</th>
<th>Level 1 (Warning)</th>
<th>Level 2 (Informational)</th>
<th>Level 3 (Debug)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Setup</td>
<td>EMERGENCY</td>
<td>CRITICAL</td>
<td>WARNING</td>
<td>DEBUG</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Process</th>
<th>Level 0 (Default - Error)</th>
<th>Level 1 (Warning)</th>
<th>Level 2 (Informational)</th>
<th>Level 3 (Debug)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnostic Framework</td>
<td>Info</td>
<td>Info</td>
<td>Info</td>
<td>Debug</td>
<td></td>
</tr>
</tbody>
</table>

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.
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:

- CTI OS Server
- OPC-CCE
- OPC-TDM
- CTISVR
- EAGTPIM
- JTAPIGATEWAY
- VRUPIM

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

Dumplog

Dumplog handles the compressed EMS files and can be used in the normal 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

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.
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.)

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>`

Also, the RTTEST “watch” command is useful.

**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.
### 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):**

```plaintext
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 execute 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

```plaintext
opctest:debug /on
```

#### Diagnosing Network Transfer Issues

```plaintext
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

```plaintext
opctest:debug /on
opctest:debug /task /passthru
```

Diagnosing VRU PG Issues

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

The default is:

```plaintext
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

```plaintext
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

```plaintext
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 10: Setting Unified CCM PIM Tracing

<table>
<thead>
<tr>
<th>Command Syntax (launch)</th>
<th>Example</th>
</tr>
</thead>
</table>
| ```plaintext
C:> ProcMon <instance> <node> pim<pim number>
``` | ```plaintext
C:> ProcMon acme PG1A pim1
``` |
| Commands                | ```plaintext
>>>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 11: Setting JTAPI Gateway Tracing

<table>
<thead>
<tr>
<th>Command Syntax (launch)</th>
<th>C:&gt; ProcMon &lt;instance&gt; &lt;node&gt; jgw&lt;jtapigw number&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>C:&gt; ProcMon acme PG1A jgw1</td>
</tr>
<tr>
<td>Commands</td>
<td>&gt;&gt;&gt;trace */off</td>
</tr>
<tr>
<td></td>
<td>&gt;&gt;&gt;debug /on</td>
</tr>
</tbody>
</table>

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 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

<table>
<thead>
<tr>
<th>Registry Key</th>
<th>HKLM\SOFTWARE\Cisco Systems, Inc\ICM&lt;instance&gt;&lt;CG#A/B\EMS\CurrentVersion\Library\Processes\ctisvr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>HKLM\SOFTWARE\Cisco Systems, Inc\ICME\CG1\EMS\CurrentVersion\Library\Processes\ctisvr</td>
</tr>
<tr>
<td>Item</td>
<td>EMSTraceMask</td>
</tr>
<tr>
<td>Value</td>
<td>F0 (hex)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Registry Key</th>
<th>Example</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\SOFTWARE\Cisco Systems, Inc.\ICM&lt;instance&gt;\CTIOS\EMS\CurrentVersion\Library\Processes\ctios</td>
<td>HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\acme\CTIOS\EMS\CurrentVersion\Library\Processes\ctios</td>
<td>EMSTraceMask</td>
</tr>
<tr>
<td>Value</td>
<td>60A0F (hex)</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 0: 0x00060A0F</td>
</tr>
<tr>
<td>Level 1: 0x00240A2F</td>
</tr>
<tr>
<td>Level 2: 0x00260A2F</td>
</tr>
<tr>
<td>Level 3: 0x002E0A2F</td>
</tr>
</tbody>
</table>

Setting VRU PIM Tracing

Resetting trace levels with the Unified ICM/Unified CCE VRU Peripheral Interface Manager (PIM) is accomplishing 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

<table>
<thead>
<tr>
<th>Registry Key</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\SOFTWARE\Cisco Systems, Inc.\ICM&lt;instance&gt;\PG&lt;PG number&gt;&lt;A or B&gt;\EMS\CurrentVersion\Library\Processes\pim&lt;pim number&gt;</td>
<td>HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\acme\PG2A\EMS\CurrentVersion\Library\Processes\pim1</td>
</tr>
</tbody>
</table>
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\<inst>\<pg>\<pg number>\<a or b>\vrucap

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\<instance>\LoggerA\EMS\CurrentVersion\Library\Processes\CampaignManager

Example:

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

### How to Reset baImport Tracing

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

Registry Key:
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\<instance>\<node>\EMS\CurrentVersion\Library\Processes\<process>

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.

EMSAllLogFilesMax

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

---

**Note**

EMSLogFileMax multiplied by EMSLogFileCountMax may be greater than EMSAllLogFilesMax 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. EMSAllLogFilesMax 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\<instanceID>\RouterA\EMS\CurrentVersion\Library\Processes\rtr.

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\logfile 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 0x2000032 on a new install or upgrade, or whenever you run Web Setup.
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 107
- Live Data Performance Counters (PCCE Deployments Only), on page 135

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**

<table>
<thead>
<tr>
<th>Counter Name (Instance)</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Processor Time (_Total)</td>
<td>Performance Object</td>
<td>Processor</td>
</tr>
<tr>
<td>Type</td>
<td>Int32</td>
<td></td>
</tr>
<tr>
<td>Units (Range)</td>
<td>Percentage (0 - 100%)</td>
<td></td>
</tr>
<tr>
<td>Threshold (Green)</td>
<td>&lt; 50%</td>
<td></td>
</tr>
<tr>
<td>Threshold (Yellow)</td>
<td>50% - 60%</td>
<td></td>
</tr>
<tr>
<td>Threshold (Red)</td>
<td>&gt; 60% (sustained)</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Primary indicator of processor activity; displays the average percentage of CPU busy time observed during the sample interval.</td>
<td></td>
</tr>
<tr>
<td>Processor Queue Length</td>
<td>Performance Object</td>
<td>System</td>
</tr>
<tr>
<td>Type</td>
<td>Int32</td>
<td></td>
</tr>
<tr>
<td>Units (Range)</td>
<td># threads</td>
<td></td>
</tr>
<tr>
<td>Threshold (Green)</td>
<td>&lt; 2 * #CPUs</td>
<td></td>
</tr>
<tr>
<td>Threshold (Yellow)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threshold (Red)</td>
<td>&gt;= 2 * #CPUs (sustained)</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Counter Name (Instance)</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>Available Bytes</td>
<td>Performance Object</td>
<td>Memory</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Int32</td>
</tr>
<tr>
<td></td>
<td>Units (Range)</td>
<td>Percentage (0 - 100%)</td>
</tr>
<tr>
<td></td>
<td>Threshold (Green)</td>
<td>&gt; 30%</td>
</tr>
<tr>
<td></td>
<td>Threshold (Yellow)</td>
<td>20% - 30%</td>
</tr>
<tr>
<td></td>
<td>Threshold (Red)</td>
<td>&lt; 20%</td>
</tr>
<tr>
<td>Description</td>
<td>Amount of physical memory available to running processes; threshold values are a percentage of physical memory. This is a snapshot—not a running average. Sustained samples below 20% (available) may be indicative of a memory leak.</td>
<td></td>
</tr>
</tbody>
</table>

| Pages / sec             | Performance Object | Memory |
|                        | Type | Int32 |
|                        | Units (Range) | # page faults |
|                        | Threshold (Green) | < 10 |
|                        | Threshold (Yellow) | >= 10 |
|                        | Threshold (Red) | > 10 (s 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. |

<table>
<thead>
<tr>
<th>Avg. Disk Queue Length (_Total)</th>
<th>Performance Object</th>
<th>Physical Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Type</td>
<td>Float</td>
</tr>
<tr>
<td></td>
<td>Units (Range)</td>
<td>Average # read/write requests</td>
</tr>
<tr>
<td></td>
<td>Threshold (Green)</td>
<td>&lt; 1.5</td>
</tr>
<tr>
<td></td>
<td>Threshold (Yellow)</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Threshold (Red)</td>
<td>&gt;= 1.5 (sustained)</td>
</tr>
<tr>
<td>Description</td>
<td>Average number of both read and write requests that were queued for the selected disk during the sample interval.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>% Disk Time (_Total)</th>
<th>Performance Object</th>
<th>Physical Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Type</td>
<td>Int32</td>
</tr>
<tr>
<td></td>
<td>Units (Range)</td>
<td>Percentage (0 - 100%)</td>
</tr>
<tr>
<td></td>
<td>Threshold (Green)</td>
<td>&lt; 60%</td>
</tr>
<tr>
<td></td>
<td>Threshold (Yellow)</td>
<td>60% - 80%</td>
</tr>
<tr>
<td></td>
<td>Threshold (Red)</td>
<td>&gt; 80%</td>
</tr>
<tr>
<td>Description</td>
<td>Percentage of elapsed time that the disk drive was busy servicing read or write requests.</td>
<td></td>
</tr>
<tr>
<td>Counter Name (Instance)</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>Bytes Total/sec</td>
<td>Performance Object</td>
<td>Network Interface</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Int32</td>
</tr>
<tr>
<td></td>
<td>Units (Range)</td>
<td>Percentage (0 - 100%)</td>
</tr>
<tr>
<td></td>
<td>Threshold (Green)</td>
<td>&lt; 25%</td>
</tr>
<tr>
<td></td>
<td>Threshold (Yellow)</td>
<td>25% - 30%</td>
</tr>
<tr>
<td></td>
<td>Threshold (Red)</td>
<td>&gt; 30%</td>
</tr>
<tr>
<td>Description</td>
<td>Rate at which bytes are sent and received over each network adapter. Threshold values are a percentage of available bandwidth.</td>
<td></td>
</tr>
<tr>
<td>Output Queue Length</td>
<td>Performance Object</td>
<td>Network Interface</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Int32</td>
</tr>
<tr>
<td></td>
<td>Units (Range)</td>
<td># packets in queue</td>
</tr>
<tr>
<td></td>
<td>Threshold (Green)</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Threshold (Yellow)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Threshold (Red)</td>
<td>&gt; 1 (sustained)</td>
</tr>
<tr>
<td>Description</td>
<td>Length of the output packet queue (in packets). If too large, there are delays and the bottleneck should be found and eliminated.</td>
<td></td>
</tr>
<tr>
<td>Buffer cache hit ratio</td>
<td>Performance Object</td>
<td>SQLServer:Buffer Manager</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Int32</td>
</tr>
<tr>
<td></td>
<td>Units (Range)</td>
<td>Percentage (0 - 100%)</td>
</tr>
<tr>
<td></td>
<td>Threshold (Green)</td>
<td>&gt; 90%</td>
</tr>
<tr>
<td></td>
<td>Threshold (Yellow)</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Threshold (Red)</td>
<td>&lt; 90%</td>
</tr>
<tr>
<td>Description</td>
<td>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. This counter is typically a good indicator of whether there is sufficient RAM installed in the server. 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 2008 R2 Enterprise Edition.</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Counter Name</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Processor Time (_Total)</td>
<td>Component</td>
<td>Processor</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Int32</td>
</tr>
<tr>
<td></td>
<td>Units (Range)</td>
<td>Percentage (0 – 100%)</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>% Processor Time is the percentage of elapsed time that the processor spends to execute 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%.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Handle Count (_Total)</th>
<th>Component</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Type</td>
<td>Int32</td>
</tr>
<tr>
<td></td>
<td>Units (Range)</td>
<td># handles</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td>Counter Name</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>Page Faults / sec</td>
<td>Component</td>
<td>Memory</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Int32</td>
</tr>
<tr>
<td></td>
<td>Units (Range)</td>
<td># faults</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Committed Bytes</td>
<td>Component</td>
<td>Memory</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Int32</td>
</tr>
<tr>
<td></td>
<td>Units (Range)</td>
<td># bytes</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Pages / sec</td>
<td>Component</td>
<td>Memory</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>float</td>
</tr>
<tr>
<td></td>
<td>Units (Range)</td>
<td># pages per second</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Threads</td>
<td>Component</td>
<td>System</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Int32</td>
</tr>
<tr>
<td></td>
<td>Units (Range)</td>
<td># threads</td>
</tr>
<tr>
<td>Description</td>
<td>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 execute instructions in a processor.</td>
<td></td>
</tr>
</tbody>
</table>
### Processor Queue Length

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>System</td>
</tr>
<tr>
<td>Type</td>
<td>Int32</td>
</tr>
<tr>
<td>Units (Range)</td>
<td># threads</td>
</tr>
</tbody>
</table>

**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 normally acceptable, dependent on the workload.

### Processes

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>System</td>
</tr>
<tr>
<td>Type</td>
<td>Int32</td>
</tr>
<tr>
<td>Units (Range)</td>
<td># processes</td>
</tr>
</tbody>
</table>

**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:)

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Physical Disk</td>
</tr>
<tr>
<td>Type</td>
<td>Float</td>
</tr>
<tr>
<td>Units (Range)</td>
<td>Percentage (0 - 100%)</td>
</tr>
</tbody>
</table>

**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:)

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Physical Disk</td>
</tr>
<tr>
<td>Type</td>
<td>Float</td>
</tr>
<tr>
<td>Units (Range)</td>
<td>Percentage (0 - 100%)</td>
</tr>
</tbody>
</table>

**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 `Error`, but this has no adverse effect on the component itself.
<table>
<thead>
<tr>
<th>Counter Name</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg. Disk Queue Length (0 C:)</td>
<td>Component</td>
<td>Physical Disk</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Float</td>
</tr>
<tr>
<td></td>
<td>Units</td>
<td># requests</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avg. Disk Queue Length (0 C:)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avg. Disk Queue Length (1 E:)</td>
<td>Component</td>
<td>Physical Disk</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Float</td>
</tr>
<tr>
<td></td>
<td>Units (Range)</td>
<td># requests</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avg. Disk Queue Length (1 E:)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avg. Disk sec/Read (0 C:)</td>
<td>Component</td>
<td>Physical Disk</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Float</td>
</tr>
<tr>
<td></td>
<td>Units</td>
<td>seconds</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avg. Disk sec/Read (0 C:)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avg. Disk sec/Read (1 E:)</td>
<td>Component</td>
<td>Physical Disk</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Float</td>
</tr>
<tr>
<td></td>
<td>Units</td>
<td>seconds</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avg. Disk sec/Read (1 E:)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: This instance is for the virtual machine's drive C—the drive where the software is installed and where logs are stored.

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 Error, 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 2008 R2, 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 17: Diagnostic Counters - All Components

<table>
<thead>
<tr>
<th>Performance Object</th>
<th>Instance</th>
<th>Counter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogicalDisk</td>
<td>_Total</td>
<td>Avg. Disk Queue Length</td>
</tr>
<tr>
<td>LogicalDisk</td>
<td>C:</td>
<td>Avg. Disk Queue Length</td>
</tr>
<tr>
<td>LogicalDisk</td>
<td>&lt;&gt;</td>
<td>Avg. Disk Queue Length</td>
</tr>
<tr>
<td>Network Interface</td>
<td>&lt;NIC Name&gt;</td>
<td>Packets Outbound Discarded</td>
</tr>
<tr>
<td>PhysicalDisk</td>
<td>_Total</td>
<td>Disk Transfers / sec</td>
</tr>
<tr>
<td>Process</td>
<td>_Total</td>
<td>Page Faults / sec</td>
</tr>
</tbody>
</table>
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 not sufficient resolution, decrease to a 5 second interval.

**Table 18: Diagnostic Counters - Logger, Administration & Data Server, and HDS**

<table>
<thead>
<tr>
<th>Performance Object</th>
<th>Instance</th>
<th>Counter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>_Total</td>
<td>Virtual Bytes</td>
</tr>
<tr>
<td>Process</td>
<td>_Total</td>
<td>Working Set</td>
</tr>
<tr>
<td>Processor</td>
<td>_Total</td>
<td>Interrupts / sec</td>
</tr>
<tr>
<td>Process</td>
<td>&lt;virus scanner&gt;</td>
<td>% Processor Time</td>
</tr>
<tr>
<td>Process</td>
<td>&lt;virus scanner&gt;</td>
<td>Page Faults / sec</td>
</tr>
<tr>
<td>Process</td>
<td>&lt;virus scanner&gt;</td>
<td>Virtual Bytes</td>
</tr>
<tr>
<td>Process</td>
<td>&lt;virus scanner&gt;</td>
<td>Working Set</td>
</tr>
</tbody>
</table>

**Logger Processes:** configlogger, histlogger, recovery, replication

**AW/HDS Processes:** configlogger, recovery, 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 not sufficient resolution, decreases to a 5 second interval.

Table 19: Diagnostic Counters - SQL Server

<table>
<thead>
<tr>
<th>Performance Object</th>
<th>Instance</th>
<th>Counter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server: Access Methods</td>
<td></td>
<td>Full Scans / sec</td>
</tr>
<tr>
<td>SQL Server: Buffer Manager</td>
<td></td>
<td>Buffer cache hit ratio</td>
</tr>
<tr>
<td>SQL Server: Buffer Manager</td>
<td></td>
<td>Page reads / sec</td>
</tr>
<tr>
<td>SQL Server: Buffer Manager</td>
<td></td>
<td>Page writes / sec</td>
</tr>
<tr>
<td>SQL Server: Buffer Manager</td>
<td></td>
<td>Stolen pages</td>
</tr>
<tr>
<td>SQL Server: Databases</td>
<td>_Total</td>
<td>Transactions / sec</td>
</tr>
<tr>
<td>SQL Server: Databases</td>
<td>csco_awdb</td>
<td>Transactions / sec</td>
</tr>
<tr>
<td>SQL Server: Databases</td>
<td>csco_hds</td>
<td>Transactions / sec</td>
</tr>
<tr>
<td>SQL Server: General Statistics</td>
<td></td>
<td>User Connections</td>
</tr>
<tr>
<td>SQL Server: Latches</td>
<td></td>
<td>Average Latch Wait Time (ms)</td>
</tr>
<tr>
<td>SQL Server: Locks</td>
<td>_Total</td>
<td>Lock Timeouts / sec</td>
</tr>
<tr>
<td>SQL Server: Locks</td>
<td>_Total</td>
<td>Number of Deadlocks / sec</td>
</tr>
<tr>
<td>SQL Server: Memory Manager</td>
<td></td>
<td>Memory Grants Pending</td>
</tr>
</tbody>
</table>

1 Where “csco” is the Unified ICM/Unified CCE instance name.
2 Where “csco” 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 20: Calculating PERF_COUNTER_COUNTER or PERF_COUNTER_BULK_COUNT

<table>
<thead>
<tr>
<th>PERF_COUNTER_COUNTER= (N1 - N0) / ((D1 - D0) / F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numerator (N)</td>
</tr>
<tr>
<td>Denominator (D)</td>
</tr>
<tr>
<td>F</td>
</tr>
</tbody>
</table>

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 21: Router Performance Counters**

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Agents Logged On*</td>
<td>The number of (contact center) agents currently logged in.</td>
</tr>
<tr>
<td>Y</td>
<td>Calls In Progress*</td>
<td>The number of calls currently in progress (being controlled by the CCE application).</td>
</tr>
<tr>
<td>Y</td>
<td>Calls/sec*</td>
<td>The (calculated) inbound call rate measured in the number of calls received per second.</td>
</tr>
<tr>
<td>Y</td>
<td>Calls In Queue</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Calls In Router</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CSNRequestsPerSec</td>
<td>Contact share node requests a second.</td>
</tr>
<tr>
<td>Y</td>
<td>CSNRequestsAvgRespTime</td>
<td>Average contact share request response time in ms.</td>
</tr>
<tr>
<td>Y</td>
<td>CSNNumberSGUpdates</td>
<td>Total Number of SG updates from target CCE systems at every live data published interval (default 3 sec).</td>
</tr>
<tr>
<td>Y</td>
<td>CSNNumberPQUpdates</td>
<td>Total Number of PQ updates from target CCE systems at every live data published interval (default 3 sec).</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Y</td>
<td>Pending PQ Count</td>
<td>Total number of precision queue configuration operations in the system yet to be fully processed.</td>
</tr>
<tr>
<td>Y</td>
<td>Pending PQ Agent Count</td>
<td>Total number of agents yet to be evaluated or handled following one or more precision queue configuration operations.</td>
</tr>
<tr>
<td>Y</td>
<td>Average PQ Update Time</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>Size</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>Messages Processed/sec</td>
<td>The number of MDS messages Router processed. By default, this counter is disabled.</td>
</tr>
<tr>
<td>N</td>
<td>Bytes Processed/sec</td>
<td>The rate of the data bytes the Router processed. By default, this counter is disabled.</td>
</tr>
<tr>
<td>N</td>
<td>Avg Process Time/Message (ms)</td>
<td>The average time (in milliseconds) the Router spends processing a MDS message.</td>
</tr>
<tr>
<td>N</td>
<td>Max Process Time(ms)</td>
<td>The maximum time (in milliseconds) the Router spends processing a MDS message.</td>
</tr>
</tbody>
</table>

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 22: Logger Performance Counters

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Number of DB Write Records</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Administration & Data Server

#### Performance Object
Cisco ICM Distributor RealTime

#### Counter Instance
{Instance Name} ADS#

#### Table 23: Administration & Data Server Real-Time Counter

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>DB Write Average Time</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>DB Write Records Processed</td>
<td>The number of records processed – written to the database – in the Historical Logger Process in the past second.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Agent Queue Depth</td>
<td>The queue depth – number of pending write transactions – for the Agent table in the Real-time Client process.</td>
</tr>
<tr>
<td>Y</td>
<td>Agent DB Write Average Time</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Agent DB Write Records Processed</td>
<td>The number of Agent table records written by the Real-time Client process in the past 1 second interval.</td>
</tr>
<tr>
<td>Y</td>
<td>Agent Skill Group Queue Depth</td>
<td>The queue depth – number of pending write transactions – for the Agent Skill Group table in the Real-time Client process.</td>
</tr>
<tr>
<td>Y</td>
<td>Agent Skill Group DB Write Average Time</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Agent Skill Group DB Write Records Processed</td>
<td>The number of Agent Skill Group table records written by the Real-time Client process in the past 1 second interval.</td>
</tr>
<tr>
<td>Y</td>
<td>Skill Group Queue Depth</td>
<td>The queue depth – number of pending write transactions – for the Skill Group table in the Real-time Client process.</td>
</tr>
<tr>
<td>Y</td>
<td>Skill Group DB Write Average Time</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Skill Group DB Write Records Processed</td>
<td>The number of Skill Group table records written by the Real-time Client process in the past 1 second interval.</td>
</tr>
<tr>
<td>Y</td>
<td>CallType Queue Depth</td>
<td>The queue depth – number of pending write transactions – for the CallType table in the Real-time Client process.</td>
</tr>
<tr>
<td>Y</td>
<td>CallType DB Write Average Time</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Performance Object

Cisco ICM Distributor Replication

**Counter Instance**

{Instance Name} Distributor #

**Table 24: Administration & Data Server Replication Counters**

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>CallType DB Write Records Processed</td>
<td>The number of CallType table records written by the Real-time Client process in the past 1 second interval.</td>
</tr>
<tr>
<td>Y</td>
<td>Route Queue Depth</td>
<td>The queue depth – number of pending write transactions – for the Route table in the Real-time Client process.</td>
</tr>
<tr>
<td>Y</td>
<td>Route DB Write Average Time</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Route DB Write Records Processed</td>
<td>The number of Route table records written by the Real-time Client process in the past 1 second interval.</td>
</tr>
<tr>
<td>Y</td>
<td>Service Queue Depth</td>
<td>The queue depth – number of pending write transactions – for the Service table in the Real-time Client process.</td>
</tr>
<tr>
<td>Y</td>
<td>Service DB Write Average Time</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Service DB Write Records Processed</td>
<td>The number of Service table records written by the Real-time Client process in the past 1 second interval.</td>
</tr>
</tbody>
</table>

### Performance Counters

**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 25: PG - OPC Counters**

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Call Count</td>
<td>Number of Calls that are currently active.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>N</td>
<td>Agent Count</td>
<td>An Agent is a specific individual who receives calls through the peripheral. This counter provides the information about the number of Agents that are configured in the system.</td>
</tr>
<tr>
<td>N</td>
<td>Skill Group Count</td>
<td>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. This counter gives the number of various skill groups available for the agents to sign in.</td>
</tr>
<tr>
<td>N</td>
<td>Services Count</td>
<td>A service is a type of processing 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. This counter gives the number of services that are configured to process the calls.</td>
</tr>
<tr>
<td>Y</td>
<td>Logged-In Agent Count</td>
<td>This counter gives the number of agents that have logged in. This does not necessarily indicate that the agents are ready to accept calls.</td>
</tr>
<tr>
<td>Y</td>
<td>Ready Agent Count</td>
<td>Number of Agents that are logged in and are ready to accept calls.</td>
</tr>
<tr>
<td>N</td>
<td>Not-Ready Agent Count</td>
<td>Number of Agents that are logged in, but occupied with task other than accepting incoming calls.</td>
</tr>
<tr>
<td>Y</td>
<td>Talking Agent Count</td>
<td>Number of Agents currently talking on Inbound or Outbound calls.</td>
</tr>
<tr>
<td>N</td>
<td>Held Agent Count</td>
<td>Number of Agents that are inactively participating in a call.</td>
</tr>
<tr>
<td>N</td>
<td>Work-Ready Agent Count</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>Work-Not-Ready Agent Count</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>Logged-Out Agent Count</td>
<td>Number of Agents that are logged out of the system. This count helps in validating the statistics if there are any state mismatches.</td>
</tr>
<tr>
<td>N</td>
<td>None-State Call Count</td>
<td>This count gives the number of calls for which a call object was created but no activity.</td>
</tr>
<tr>
<td>N</td>
<td>Null-State Call Count</td>
<td>This count gives the number of calls that has no relationship between the call and device.</td>
</tr>
<tr>
<td>N</td>
<td>Initiated Call Count</td>
<td>This count gives the number of calls for which the device has requested for a service. Often this is the dialing state.</td>
</tr>
<tr>
<td>N</td>
<td>Alerting Call Count</td>
<td>This count gives 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.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Y</td>
<td>Connected Call Count</td>
<td>This count gives the number of calls for which the device is actively participating in the call.</td>
</tr>
<tr>
<td>N</td>
<td>Held Call Count</td>
<td>This count gives the number of calls for which the device is inactively participating in the call.</td>
</tr>
<tr>
<td>N</td>
<td>Queued Call Count</td>
<td>This count gives the number of calls for which the normal 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.</td>
</tr>
<tr>
<td>N</td>
<td>Failed Call Count</td>
<td>This count gives the number of calls for which the normal state progression has been aborted. 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.</td>
</tr>
</tbody>
</table>

**Enable optional counters**

**Key**

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<Instance>\<PG#>\PG\CurrentVersion\OPC
```

**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 26: PG - CM PIM Counters**

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

**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**
```
"{InstanceName}PG#A/B PIM#" (For example, “acme PG3A PIM3")
```

**Table 27: PG - VRU PIM Counters**

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Calls At VRU</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>Messages To VRU/sec</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>Messages From VRU/sec</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>Bytes To VRU/sec</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>Bytes From VRU/sec</td>
<td>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.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Y</td>
<td>New Calls/sec</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Pre-Routed Calls/Sec</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Connection Resets</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 28: CTI Server Counters**

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>Reported Call Count</td>
<td>Number of calls that are already reported to the CTI clients.</td>
</tr>
<tr>
<td>N</td>
<td>Active Call Count</td>
<td>Number of calls that are currently in progress.</td>
</tr>
<tr>
<td>N</td>
<td>Deactivated Call Count</td>
<td>Number of calls that are not currently active and eventually cleared.</td>
</tr>
<tr>
<td>N</td>
<td>Cleared Call Count</td>
<td>Number of calls that no longer exist in the system.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>N</td>
<td>Private Call Count</td>
<td>Number of calls that are privately tracked by CTI Server and which are not reported to OPC.</td>
</tr>
<tr>
<td>Y</td>
<td>Logged-In Agent Count</td>
<td>Agents that have logged in. This does not necessarily indicate that they are ready to accept calls.</td>
</tr>
<tr>
<td>Y</td>
<td>Ready Agent Count</td>
<td>Number of Agents that are logged in and ready to accept calls.</td>
</tr>
<tr>
<td>N</td>
<td>Not-Ready Agent Count</td>
<td>Number of Agents that are logged in, but occupied with tasks other than accepting incoming calls.</td>
</tr>
<tr>
<td>Y</td>
<td>Talking Agent Count</td>
<td>Number of Agents currently talking on Inbound or Outbound calls.</td>
</tr>
<tr>
<td>N</td>
<td>Held Agent Count</td>
<td>Number of Agents that are inactively participating in a call.</td>
</tr>
<tr>
<td>N</td>
<td>Work-Ready Agent Count</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>Work-Not-Ready Agent Count</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>Logged-Out Agent Count</td>
<td>The number of Agents that are logged out of the system. This count helps in validating the statistics if there are any state mismatches.</td>
</tr>
<tr>
<td>Y</td>
<td>Sessions Unknown</td>
<td>The number of sessions for which there is no socket connection made yet.</td>
</tr>
<tr>
<td>N</td>
<td>Sessions Opening</td>
<td>The number of sessions that are in the process of setting up a connection.</td>
</tr>
<tr>
<td>Y</td>
<td>Sessions Open</td>
<td>The number of sessions that were successfully setup.</td>
</tr>
<tr>
<td>N</td>
<td>Sessions Closing</td>
<td>The number of sessions that are in the process of tear down.</td>
</tr>
<tr>
<td>Y</td>
<td>Sessions Closed</td>
<td>The total number of sessions that are terminated by the CTI Server.</td>
</tr>
<tr>
<td>Y</td>
<td>Sessions Failed</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Total Sessions</td>
<td>The total number of sessions maintained by CTI Server.</td>
</tr>
</tbody>
</table>

**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 29: CTI OS Server Counters

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>CTI OS Active Client Connections</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS Active Monitor Mode Connections</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS Active Calls</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS Configured Skill Groups</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS Configured Teams</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS Configured Agents</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS Active Conferences</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS Call Count</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS Conference Count</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS Transfer Count</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS Call Failed Count</td>
<td>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.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS CTI Message Receive Rate (msg/sec)</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS CTI Message Send Rate (msg/sec)</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS Service Broker Queue Size</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>CTI OS Call Object Count</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>CTI OS Connection Object Count</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>CTI OS Argument Object Count</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>CTI OS Device Object Count</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>CTI OS Agent Object Count</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>CTI OS Skill group Object Count</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>CTI OS Supervisor Object Count</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>CTI OS Team Object Count</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>CTI OS Total Objects Created Count</td>
<td>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.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>N</td>
<td>CTI OS Total Objects Deletion Count</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>CTI OS Active Object Count</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS CLIENT Send Message Rate (msg/sec)</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS CLIENT Receive Message Rate (msg/sec)</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS CLIENT Total Number of Pending Write Operations</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS CLIENT Total Message Buffer Size (Bytes)</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>CTI OS CG Receive Queue Size</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 30: Outbound Option Campaign Manager Counters

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>DB Space Utilization</td>
<td>The Campaign Manager and Import processes share a private database on the Side A 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%).</td>
</tr>
<tr>
<td>Y</td>
<td>Queue Depth</td>
<td>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. The Campaign Manager will deliberately restart when this value exceeds the limit of 10,000 messages in queue.</td>
</tr>
<tr>
<td>Y</td>
<td>Average Queue Time</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Do Not Call Number Count</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Active Dialer Count</td>
<td>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.</td>
</tr>
</tbody>
</table>

Outbound Option Import

Performance Object
Cisco ICM Import

Counter Instance
“{Instance Name}”

Table 31: Outbound Option Import Counters

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Records Imported Today</td>
<td>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.</td>
</tr>
</tbody>
</table>

Outbound Option Dialer

Performance Object
Cisco ICM Dialer
### Counter Instance

“{Instance Name}”

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Queue Depth</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Average Queue Time</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Talking Agents</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Busy Port (Customer) Count</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Busy Port (Reservation) Count</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Idle Port Count</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Call Attempt Count</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Abandoned Call Count</td>
<td>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 all 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.</td>
</tr>
<tr>
<td>Y</td>
<td>Reservation Call Count</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Answering Machine Call Count</td>
<td>A campaign can be enabled to differentiate between live voice and answering machines. This counter tracks how many answering machines were detected today.</td>
</tr>
<tr>
<td>Y</td>
<td>Customer Answered Call Count</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Customer Not Answered Call Count</td>
<td>The Dialer attempts to contact customers. This counter tracks how many attempts resulted in no answer condition. This counter is reset daily.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Y</td>
<td>Error Call Count</td>
<td>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.</td>
</tr>
<tr>
<td>Y</td>
<td>Number of attempted calls per second</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Message Delivery Service

**Performance Object**
Cisco ICM MDSCLIENT

**Counter Instance**
"{Instance Name}"  

**Table 33: MDS Client Counters**

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>Client Handle ID</td>
<td>Handle for this MDS client. It is used to uniquely identify the MDS client connected to the MDS process.</td>
</tr>
<tr>
<td>N</td>
<td>Now Message Received</td>
<td>Number of messages received by the MDS client per second.</td>
</tr>
<tr>
<td>N</td>
<td>Now Message Sent</td>
<td>Number of messages sent by the MDS client per second.</td>
</tr>
<tr>
<td>N</td>
<td>Now Bytes Received</td>
<td>Number of bytes received by the MDS client per second.</td>
</tr>
<tr>
<td>N</td>
<td>Now Bytes Sent</td>
<td>Number of bytes sent by the MDS client per second.</td>
</tr>
<tr>
<td>N</td>
<td>Current Buffers Memory Allocated</td>
<td>Total number of bytes used by all currently allocated buffers.</td>
</tr>
<tr>
<td>N</td>
<td>Current Buffers Allocated</td>
<td>Total number of buffers currently allocated from buffer pool.</td>
</tr>
<tr>
<td>N</td>
<td>Buffers Allocation Requests/sec</td>
<td>Number of buffers allocated per second.</td>
</tr>
<tr>
<td>N</td>
<td>Buffers Free Requests/sec</td>
<td>Number of buffers freed per second.</td>
</tr>
<tr>
<td>N</td>
<td>Current Buffers Memory Limit</td>
<td>Maximum amount of memory allowed to be allocated for buffers for this process.</td>
</tr>
<tr>
<td>N</td>
<td>Initial Buffers Memory Limit</td>
<td>Amount of memory limit reserved for buffers for this process.</td>
</tr>
<tr>
<td>N</td>
<td>SendClientQ Current Depth</td>
<td>Current number of messages in the MDS Client Send Queue.</td>
</tr>
<tr>
<td>N</td>
<td>SendClientQ Now Messages In/sec</td>
<td>Total number of messages added to the MDS Client Send Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>SendClientQ Now Messages Out/sec</td>
<td>Total number of messages removed from the MDS Client Send Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>SendClientQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the MDS Client Send Queue per second.</td>
</tr>
</tbody>
</table>
### Performance Counters

**Counter Instance**

```
"{Instance name}"  
```

### Table 34: MDS Process Client Counters

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>SendClientQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the MDS Client Send Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>SendClientQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the MDS Client Send Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>SendClientQ Avg. Queue Response Time [ms]</td>
<td>Average time in milliseconds a message waits in the MDS Client Send Queue.</td>
</tr>
<tr>
<td>N</td>
<td>SendClientQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the MDS Client Send Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>Client Handle ID</td>
<td>Handle for this MDS client. It is used to uniquely identify the MDS client connected to the MDS process.</td>
</tr>
<tr>
<td>N</td>
<td>Total MDS Client Connects</td>
<td>Total number of times the MDS client has connected to the MDS process.</td>
</tr>
<tr>
<td>N</td>
<td>Total MDS Client Disconnects</td>
<td>Total number of times the MDS client has disconnected from the MDS process.</td>
</tr>
<tr>
<td>N</td>
<td>Now Message Received from Client</td>
<td>Number of messages received from the MDS client per second.</td>
</tr>
<tr>
<td>N</td>
<td>Now Message Sent to Client</td>
<td>Number of messages sent to the MDS client per second.</td>
</tr>
<tr>
<td>N</td>
<td>Now Bytes Received from Client</td>
<td>Number of bytes received from the MDS client per second.</td>
</tr>
<tr>
<td>N</td>
<td>Now Bytes Sent to Client</td>
<td>Number of bytes sent to the MDS client per second.</td>
</tr>
<tr>
<td>N</td>
<td>ToClientQ Current Depth</td>
<td>Current number of messages in the MDS Send Client Queue.</td>
</tr>
<tr>
<td>N</td>
<td>ToClientQ Now Messages In/sec</td>
<td>Total number of messages added to the MDS Client Send Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>ToClientQ Now Messages Out/sec</td>
<td>Total number of messages removed from the MDS Client Send Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>ToClientQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the MDS Client Send Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>ToClientQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the MDS Client Send Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>ToClientQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the MDS Client Send Queue per second.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>N</td>
<td>ToClientQ Avg. Queue Response Time [ms]</td>
<td>Average time in milliseconds a message waits in the MDS Client Send Queue.</td>
</tr>
<tr>
<td>N</td>
<td>ToClientQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the MDS Client Send Queue experience.</td>
</tr>
</tbody>
</table>

**Performance Object**
Cisco ICM MDSPROC

**Counter Instance**
“{Instance Name}”

**Table 35: MDS Process Counters**

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>Current Buffers Memory Allocated</td>
<td>Total number of bytes used by all currently allocated buffers.</td>
</tr>
<tr>
<td>N</td>
<td>Current Buffers Allocated</td>
<td>Total number of buffers currently allocated from buffer pool.</td>
</tr>
<tr>
<td>N</td>
<td>Buffers Allocation Requests/sec</td>
<td>Number of buffers allocated per second.</td>
</tr>
<tr>
<td>N</td>
<td>Buffers Free Requests/sec</td>
<td>Number of buffers freed per second.</td>
</tr>
<tr>
<td>N</td>
<td>Current Buffers Memory Limit</td>
<td>Maximum amount of memory allowed to be allocated for buffers for this process.</td>
</tr>
<tr>
<td>N</td>
<td>Initial Buffers Memory Limit</td>
<td>Amount of memory limit reserved for buffers for this process.</td>
</tr>
<tr>
<td>N</td>
<td>Synch Messages Ordered/sec</td>
<td>Number of messages ordered by the MDS synchronizer per second.</td>
</tr>
<tr>
<td>N</td>
<td>Synch MDS Duplicates/sec</td>
<td>Number of duplicate MDS messages detected by the synchronizer per second.</td>
</tr>
<tr>
<td>N</td>
<td>Synch DMP Duplicates/sec</td>
<td>Number of duplicate DMP messages detected by the synchronizer per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighInQ Current Depth</td>
<td>Current number of messages in the Local High Incoming Queue.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighInQ Now Messages In/sec</td>
<td>Total number of messages added to the Local High Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighInQ Now Messages Out/sec</td>
<td>Total number of messages removed from the Local High Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighInQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Local High Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighInQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Local High Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighInQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Local High Incoming Queue per second.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighInQ Avg. Queue Response Time [ms]</td>
<td>Average time in milliseconds a message waits in the Local High Incoming Queue.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighInQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Local High Incoming Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedInQ Current Depth</td>
<td>Current number of messages in the Local Medium Incoming Queue.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedInQ Now Messages In/sec</td>
<td>Total number of messages added to the Local Medium Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedInQ Now Messages Out/sec</td>
<td>Total number of messages removed from the Local Medium Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedInQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Local Medium Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedInQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Local Medium Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedInQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Local Medium Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedInQ Avg. Queue Response Time [ms]</td>
<td>Average time in milliseconds a message waits in the Local Medium Incoming Queue.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedInQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Local Medium Incoming Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowInQ Current Depth</td>
<td>Current number of messages in the Local Low Incoming Queue.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowInQ Now Messages In/sec</td>
<td>Total number of messages added to the Local Low Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowInQ Now Messages Out/sec</td>
<td>Total number of messages removed from the Local Low Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowInQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Local Low Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowInQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Local Low Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowInQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Local Low Incoming Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowInQ Avg. Queue Response Time [ms]</td>
<td>Average time in milliseconds a message waits in the Local Low Incoming Queue.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowInQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Local Low Incoming Queue experience.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOutQ Current Depth</td>
<td>Current number of messages in the Remote High Output Queue.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOutQ Now Messages In/sec</td>
<td>Total number of messages added to the Remote High Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOutQ Now Messages Out/sec</td>
<td>Total number of messages removed from the Remote High Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOutQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Remote High Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOutQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Remote High Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOutQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Remote High Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOutQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Remote High Output Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOutQ Current Depth</td>
<td>Current number of messages in the Remote Medium Output Queue.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOutQ Now Messages In/sec</td>
<td>Total number of messages added to the Remote Medium Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOutQ Now Messages Out/sec</td>
<td>Total number of messages removed from the Remote Medium Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOutQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Remote Medium Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOutQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Remote Medium Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOutQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Remote Medium Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOutQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Remote Medium Output Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOutQ Current Depth</td>
<td>Current number of messages in the Remote Low Output Queue.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOutQ Now Messages In/sec</td>
<td>Total number of messages added to the Remote Low Output Queue per second.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOutQ Now Messages Out/sec</td>
<td>Total number of messages removed from the Remote Low Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOutQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Remote Low Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOutQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Remote Low Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOutQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Remote Low Output Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOutQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Remote Low Output Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighOrderQ Current Depth</td>
<td>Current number of messages in the Local High Order Queue.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighOrderQ Now Messages In/sec</td>
<td>Total number of messages added to the Local High Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighOrderQ Now Messages Out/sec</td>
<td>Total number of messages removed from the Local High Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighOrderQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Local High Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighOrderQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Local High Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighOrderQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Local High Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighOrderQ Avg. Queue Response Time [ms]</td>
<td>Average time in milliseconds a message waits in the Local High Order Queue.</td>
</tr>
<tr>
<td>N</td>
<td>LocalHighOrderQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Local High Order Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedOrderQ Current Depth</td>
<td>Current number of messages in the Local Medium Order Queue.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedOrderQ Now Messages In/sec</td>
<td>Total number of messages added to the Local Medium Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedOrderQ Now Messages Out/sec</td>
<td>Total number of messages removed from the Local Medium Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedOrderQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Local Medium Order Queue per second.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedOrderQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Local Medium Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedOrderQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Local Medium Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedOrderQ Avg. Queue Response Time [ms]</td>
<td>Average time in milliseconds a message waits in the Local Medium Order Queue.</td>
</tr>
<tr>
<td>N</td>
<td>LocalMedOrderQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Local Medium Order Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowOrderQ Current Depth</td>
<td>Current number of messages in the Local Low Order Queue.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowOrderQ Now Messages In/sec</td>
<td>Total number of messages added to the Local Low Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowOrderQ Now Messages Out/sec</td>
<td>Total number of messages removed from the Local Low Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowOrderQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Local Low Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowOrderQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Local Low Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowOrderQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Local Low Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowOrderQ Avg. Queue Response Time [ms]</td>
<td>Average time in milliseconds a message waits in the Local Low Order Queue.</td>
</tr>
<tr>
<td>N</td>
<td>LocalLowOrderQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Local Low Order Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOrderQ Current Depth</td>
<td>Current number of messages in the Remote High Order Queue.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOrderQ Now Messages In/sec</td>
<td>Total number of messages added to the Remote High Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOrderQ Now Messages Out/sec</td>
<td>Total number of messages removed from the Remote High Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOrderQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Remote High Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOrderQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Remote High Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOrderQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Remote High Order Queue per second.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>N</td>
<td>RemoteHighOrderQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Remote High Order Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOrderQ Current Depth</td>
<td>Current number of messages in the Remote Medium Order Queue.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOrderQ Avg. Message In/sec</td>
<td>Total number of messages added to the Remote Medium Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOrderQ Avg. Message Out/sec</td>
<td>Total number of messages removed from the Remote Medium Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOrderQ Avg. Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Remote Medium Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOrderQ Avg. Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Remote Medium Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOrderQ Avg. Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Remote Medium Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteMedOrderQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Remote Medium Order Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOrderQ Current Depth</td>
<td>Current number of messages in the Remote Low Order Queue.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOrderQ Avg. Message In/sec</td>
<td>Total number of messages added to the Remote Low Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOrderQ Avg. Message Out/sec</td>
<td>Total number of messages removed from the Remote Low Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOrderQ Avg. Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Remote Low Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOrderQ Avg. Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Remote Low Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOrderQ Avg. Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Remote Low Order Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOrderQ Avg. Queue Response Time [ms]</td>
<td>Average time in milliseconds a message waits in the Remote Low Order Queue.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>N</td>
<td>RemoteLowOrderQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Remote Low Order Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>TDHighQ Current Depth</td>
<td>Current number of messages in the Timed Delivery High Queue.</td>
</tr>
<tr>
<td>N</td>
<td>TDHighQ Now Messages In/sec</td>
<td>Total number of messages added to the Timed Delivery High Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDHighQ Now Messages Out/sec</td>
<td>Total number of messages removed from the Timed Delivery High Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDHighQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Timed Delivery High Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDHighQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Timed Delivery High Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDHighQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Timed Delivery High Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDHighQ Avg. Queue Response Time [ms]</td>
<td>Average time in milliseconds a message waits in the Timed Delivery High Queue.</td>
</tr>
<tr>
<td>N</td>
<td>TDHighQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Timed Delivery High Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>TDMedQ Current Depth</td>
<td>Current number of messages in the Timed Delivery Medium Queue.</td>
</tr>
<tr>
<td>N</td>
<td>TDMedQ Now Messages In/sec</td>
<td>Total number of messages added to the Timed Delivery Medium Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDMedQ Now Messages Out/sec</td>
<td>Total number of messages removed from the Timed Delivery Medium Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDMedQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Timed Delivery Medium Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDMedQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Timed Delivery Medium Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDMedQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Timed Delivery Medium Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDMedQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Timed Delivery Medium Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>TDLowQ Current Depth</td>
<td>Current number of messages in the Timed Delivery Low Queue.</td>
</tr>
<tr>
<td>N</td>
<td>TDLowQ Now Messages In/sec</td>
<td>Total number of messages added to the Timed Delivery Low Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDLowQ Now Messages Out/sec</td>
<td>Total number of messages removed from the Timed Delivery Low Queue per second.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>N</td>
<td>TDLowQ Now Bytes In/sec</td>
<td>Total number of bytes added for all messages to the Timed Delivery Low Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDLowQ Now Bytes Out/sec</td>
<td>Total number of bytes removed for all the messages from the Timed Delivery Low Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDLowQ Now Traffic Intensity</td>
<td>Ratio of the number of messages added to the number of messages removed from the Timed Delivery Low Queue per second.</td>
</tr>
<tr>
<td>N</td>
<td>TDLowQ Avg. Queue Response Time [ms]</td>
<td>Average time in milliseconds a message waits in the Timed Delivery Low Queue.</td>
</tr>
<tr>
<td>N</td>
<td>TDLowQ 90% Queue Response Time [ms]</td>
<td>The response time in milliseconds that 90% of all messages passing through the Timed Delivery Low Queue experience.</td>
</tr>
<tr>
<td>N</td>
<td>Output Waits</td>
<td>Total number of times output from critical client (Route or OPC) waited for ACK from MDS peer.</td>
</tr>
<tr>
<td>N</td>
<td>Average Output Wait Time</td>
<td>Average number of milliseconds MDS output waits to receive an ACK message from MDS peer.</td>
</tr>
<tr>
<td>N</td>
<td>Private Net Min RTT</td>
<td>Minimum time it took MDS to send a message over the private network and receive an ACK response from MDS peer.</td>
</tr>
<tr>
<td>N</td>
<td>Private Net Avg RTT</td>
<td>Average time it took MDS to send a message over the private network and receive an ACK response from MDS peer.</td>
</tr>
<tr>
<td>N</td>
<td>Private Net Max RTT</td>
<td>Maximum time it took MDS to send a message over the private network and receive an ACK response from MDS peer.</td>
</tr>
</tbody>
</table>

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
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 36: Cisco ICM QoS

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>High BytesSent/sec</td>
<td>High BytesSent/sec is the number of bytes per second sent to the other side over high priority connection.</td>
</tr>
<tr>
<td>N</td>
<td>High MsgsSent/sec</td>
<td>High MsgsSent/sec is the number of messages sent to the other side over high priority connection.</td>
</tr>
<tr>
<td>N</td>
<td>High BytesRcvd/sec</td>
<td>High BytesRcvd/sec is the number of bytes received from the other side over high priority connection.</td>
</tr>
<tr>
<td>N</td>
<td>High MsgsRcvd/sec</td>
<td>High MsgsRcvd/sec is the number of messages received from the other side over high priority connection.</td>
</tr>
<tr>
<td>N</td>
<td>High LocalRttMean</td>
<td>High LocalRttMean is the mean Round Trip Time in milliseconds of high priority messages as measured by local node.</td>
</tr>
<tr>
<td>N</td>
<td>High LocalRttStdDev</td>
<td>High LocalRttStdDev is the standard deviation of Round Trip Time of high priority messages as measured by local node.</td>
</tr>
<tr>
<td>N</td>
<td>High RemoteRttMean</td>
<td>High RemoteRttMean is the mean Round Trip Time in milliseconds of high priority messages as measured by remote node.</td>
</tr>
<tr>
<td>N</td>
<td>High RemoteRttStdDev</td>
<td>High RemoteRttStdDev is the standard deviation of Round Trip Time of high priority messages as measured by remote node.</td>
</tr>
<tr>
<td>N</td>
<td>High Xmit NowQueueDepth</td>
<td>High Xmit NowQueueDepth is the current number of messages in the transmit queue for high priority traffic.</td>
</tr>
<tr>
<td>N</td>
<td>High Xmit MaxQueueDepth</td>
<td>High Xmit MaxQueueDepth is the maximum number of message observed in the transmit queue for high priority traffic.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>N</td>
<td>High Xmit NowBytesQueued</td>
<td>High Xmit NowBytesQueued is the current number of bytes in the retransmit queue for high priority traffic.</td>
</tr>
<tr>
<td>N</td>
<td>High Xmit MaxBytesQueued</td>
<td>High Xmit MaxBytesQueued is the maximum number of bytes observed in the retransmit queue for high priority traffic.</td>
</tr>
<tr>
<td>N</td>
<td>High TotalQoSReallocations</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>Med BytesSent/sec</td>
<td>Med BytesSent/sec is the number of bytes per second sent to the other side over medium priority connection.</td>
</tr>
<tr>
<td>N</td>
<td>Med BytesRcvd/sec</td>
<td>Med BytesRcvd/sec is the number of bytes received from the other side over medium priority connection.</td>
</tr>
<tr>
<td>N</td>
<td>Med MsgsSent/sec</td>
<td>Med MsgsSent/sec is the number of messages sent to the other side over medium priority connection.</td>
</tr>
<tr>
<td>N</td>
<td>Med MsgsRcvd/sec</td>
<td>Med MsgsRcvd/sec is the number of messages received from the other side over medium priority connection.</td>
</tr>
<tr>
<td>N</td>
<td>Med LocalRttMean</td>
<td>Med LocalRttMean is the mean Round Trip Time in milliseconds of medium priority messages as measured by local node.</td>
</tr>
<tr>
<td>N</td>
<td>Med LocalRttStdDev</td>
<td>Med LocalRttStdDev is the standard deviation of Round Trip Time of medium priority messages as measured by local node.</td>
</tr>
<tr>
<td>N</td>
<td>Med RemoteRttMean</td>
<td>Med RemoteRttMean is the mean Round Trip Time in milliseconds of medium priority messages as measured by remote node.</td>
</tr>
<tr>
<td>N</td>
<td>Med RemoteRttStdDev</td>
<td>Med RemoteRttStdDev is the standard deviation of Round Trip Time of medium priority messages as measured by remote node.</td>
</tr>
<tr>
<td>N</td>
<td>Med Xmit NowQueueDepth</td>
<td>Med Xmit NowQueueDepth is the current number of messages in the transmit queue for medium priority traffic.</td>
</tr>
<tr>
<td>N</td>
<td>Med Xmit MaxQueueDepth</td>
<td>Med Xmit MaxQueueDepth is the maximum number of message observed in the transmit queue for medium priority traffic.</td>
</tr>
<tr>
<td>N</td>
<td>Med Xmit NowBytesQueued</td>
<td>Med Xmit NowBytesQueued is the current number of bytes in the retransmit queue for medium priority traffic.</td>
</tr>
<tr>
<td>N</td>
<td>Med Xmit MaxBytesQueued</td>
<td>Med Xmit MaxBytesQueued is the maximum number of bytes observed in the retransmit queue for medium priority traffic.</td>
</tr>
<tr>
<td>N</td>
<td>Med TotalQoSReallocations</td>
<td>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.</td>
</tr>
<tr>
<td>N</td>
<td>Low BytesSent/sec</td>
<td>Low BytesSent/sec is the number of bytes per second sent to the other side over low priority connection.</td>
</tr>
<tr>
<td>N</td>
<td>Low MsgsSent/sec</td>
<td>Low MsgsSent/sec is the number of messages sent to the other side over low priority connection.</td>
</tr>
<tr>
<td>N</td>
<td>Low BytesRcvd/sec</td>
<td>Low BytesRcvd/sec is the number of bytes received from the other side over low priority connection.</td>
</tr>
<tr>
<td>Always ON?</td>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>N</td>
<td>Low MsgsRcvd/sec</td>
<td>Low MsgsRcvd/sec is the number of messages received from the other side over low priority connection.</td>
</tr>
<tr>
<td>N</td>
<td>Low LocalRttMean</td>
<td>Low LocalRttMean is the mean Round Trip Time in milliseconds of low priority messages as measured by local node.</td>
</tr>
<tr>
<td>N</td>
<td>Low LocalRttStdDev</td>
<td>Low LocalRttStdDev is the standard deviation of Round Trip Time of low priority messages as measured by local node.</td>
</tr>
<tr>
<td>N</td>
<td>Low RemoteRttMean</td>
<td>Low RemoteRttMean is the mean Round Trip Time in milliseconds of low priority messages as measured by remote node.</td>
</tr>
<tr>
<td>N</td>
<td>Low RemoteRttStdDev</td>
<td>Low RemoteRttStdDev is the standard deviation of Round Trip Time of low priority messages as measured by remote node.</td>
</tr>
<tr>
<td>N</td>
<td>Low Xmit NowQueueDepth</td>
<td>Low Xmit NowQueueDepth is the current number of messages in the transmit queue for low priority traffic.</td>
</tr>
<tr>
<td>N</td>
<td>Low Xmit MaxQueueDepth</td>
<td>Low Xmit MaxQueueDepth is the maximum number of message observed in the transmit queue for low priority traffic.</td>
</tr>
<tr>
<td>N</td>
<td>Low Xmit NowBytesQueued</td>
<td>Low Xmit NowBytesQueued is the current number of bytes in the retransmit queue for low priority traffic.</td>
</tr>
<tr>
<td>N</td>
<td>Low Xmit MaxBytesQueued</td>
<td>Low Xmit MaxBytesQueued is the maximum number of bytes observed in the retransmit queue for low priority traffic.</td>
</tr>
<tr>
<td>N</td>
<td>Low TotalQoSReallocations</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.
QoS Marking for Live Data (PCCE Deployments Only)

The default Unified CCE QoS markings can be overwritten if necessary. The tables below show the default markings, latency requirement, IP address, and port associated with each priority flow for the public and private network traffic respectively, where i# represents the customer instance number. Notice that in the public network the medium-priority traffic is sent with the high-priority public IP address and marked the same as the high-priority traffic, while in the private network it is sent with the non-high-priority private IP address and marked the same as the low-priority traffic.

Table 37: Public Network Traffic Markings (Default) and Latency Requirements for Live Data TIP Services

<table>
<thead>
<tr>
<th>Priority</th>
<th>Live Data Server-Side IP Address and Port</th>
<th>One-Way Latency requirement</th>
<th>DSCP / 802.1p marking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>For the TIP Event listening port settings, port 034 is used. The TIP listening port on the Router is as follows.</td>
<td>1 seconds</td>
<td>AF11 / 1</td>
</tr>
<tr>
<td></td>
<td>• Router A: 40034 + inst# * 40</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Router B: 41034 + inst# * 40</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Public Network Traffic Marking on PGs for Live Data applies only to Agent PGs. Installation of two PGs (under the same Customer Instance) on a single PG VM is supported. On a PCCE deployment, however, only one Agent PG (PG1) is supported. The TIP listening ports for PGs are as follows:

• PG#1 A: 42034 + inst# * 40
• PG#1 B: 43034 + inst# * 40
• PG#2 A: 44034 + inst# * 40
• PG#2 B: 45034 + inst# * 40

Live Data Performance Counters (PCCE Deployments Only)

The following table lists the performance counters you should watch on a regular basis to monitor activity related to Live Data reporting.

Note: Performance counter support for Live Data is available only for PCCE deployments in this release. (Support for UCCE deployments is unavailable at this time.)

Table 38: Live Data Performance Counters - Report Monitoring

Performance Object: Cisco LiveData
### Counter Instance:
- RouterA or RouterB
- PG###/A/B (for example: PG1A)

<table>
<thead>
<tr>
<th>Always ON?</th>
<th>Counter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Socket Connects</td>
<td>The number of successful socket connections made to the Live Data service running on the peer node in this reporting connection.</td>
</tr>
<tr>
<td>Y</td>
<td>Socket Disconnects</td>
<td>The number of socket disconnects with the Live Data service running on the peer node in this reporting connection.</td>
</tr>
<tr>
<td>Y</td>
<td>ConnectRequests Received</td>
<td>The number of ConnectRequest messages received.</td>
</tr>
<tr>
<td>Y</td>
<td>ConnectResponses Sent</td>
<td>The number of ConnectResponse messages sent.</td>
</tr>
<tr>
<td>Y</td>
<td>StartDataRequests Received</td>
<td>The number of StartDataRequest messages received.</td>
</tr>
<tr>
<td>Y</td>
<td>StartDataResponses Sent</td>
<td>The number of StartDataResponse messages sent.</td>
</tr>
<tr>
<td>Y</td>
<td>Output Queue Depth</td>
<td>The current output queue depth (in messages).</td>
</tr>
<tr>
<td>Y</td>
<td>Retransmit Queue Depth</td>
<td>The current retransmit queue depth (in messages).</td>
</tr>
<tr>
<td>Y</td>
<td>Messages Discarded</td>
<td>The number of messages discarded.</td>
</tr>
<tr>
<td>Y</td>
<td>Heartbeat Loss Countdown</td>
<td>The number of heartbeat response losses since the last reset connect. The connect is reset by default after five consecutive heartbeat losses.</td>
</tr>
<tr>
<td>Y</td>
<td>Missing Heartbeat Responses</td>
<td>The total number of missing heartbeat responses since startup.</td>
</tr>
<tr>
<td>Y</td>
<td>Last Sequence Number Acknowledged</td>
<td>The last sequence number acknowledged.</td>
</tr>
<tr>
<td>Y</td>
<td>Last Sequence Number Assigned</td>
<td>The last sequence number assigned.</td>
</tr>
<tr>
<td>Y</td>
<td>Active Connection</td>
<td>The active connection (1: yes, 0: no).</td>
</tr>
</tbody>
</table>
Capacity Planning

- Capacity Planning Process, on page 137
- Capacity Planning – Getting Started, on page 138
- Collected Data Categorization, on page 139
- Capacity Utilization, on page 142

Capacity Planning Process

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**: Re-execute the process the same it was done before you ensure that an equal comparison is made.

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):
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 142. 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:
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:
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 skill groups, 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 normal. 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
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 execution 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 >= 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/custcsw/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 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 39: Calculating CPU Utilization*

<table>
<thead>
<tr>
<th>Measurement Counter</th>
<th>% Processor Time (_Total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU$_{95%}$</td>
<td></td>
</tr>
<tr>
<td>CPU$_{Sat}$</td>
<td>Maximum threshold: 60%</td>
</tr>
<tr>
<td>Indicator Counter</td>
<td>Counter: System – Processor Queue Length</td>
</tr>
<tr>
<td></td>
<td>Threshold: 2 X # CPU Cores</td>
</tr>
</tbody>
</table>

**Memory Utilization Calculations**

*Table 40: Calculating Memory Utilization*

\[
\text{Mem}_{Sat} = \text{Mem}_{physical} \cdot 0.8
\]

<table>
<thead>
<tr>
<th>Measurement Counter</th>
<th>% Committed Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mem$_{95%}$</td>
<td>Threshold: 80% (of physical memory)</td>
</tr>
<tr>
<td>Mem$_{Sat}$</td>
<td>Threshold: &lt; 20%</td>
</tr>
<tr>
<td>Indicator Counters</td>
<td>Counter: Memory – Available Mbytes</td>
</tr>
<tr>
<td></td>
<td>Threshold: 20%</td>
</tr>
<tr>
<td></td>
<td>Counter: Paging File – % Usage</td>
</tr>
<tr>
<td></td>
<td>Threshold: 80%</td>
</tr>
</tbody>
</table>
Disk Utilization Calculations

Table 41: Calculating Disk Utilization

<table>
<thead>
<tr>
<th>Measurement Counter: Processor – % Processor Time (_Total)</th>
<th>DT₉₅%</th>
</tr>
</thead>
<tbody>
<tr>
<td>DT₉₅%</td>
<td>95%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Measurement Counter: Physical Disk – Avg. Disk Queue Length</th>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>DT₅₅%</td>
<td>Maximum threshold: 50%</td>
</tr>
<tr>
<td>Indicator</td>
<td>Counter: Physical Disk – Avg. Disk Queue Length</td>
</tr>
<tr>
<td>Threshold: 1.5</td>
<td>Threshold: 1.5</td>
</tr>
</tbody>
</table>

NIC Utilization Calculations

Table 42: Calculating NIC Utilization

<table>
<thead>
<tr>
<th>Measurement Counter: Network Interface – Bytes Total / sec</th>
<th>NIC₅₅%</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC₅₅%</td>
<td>95%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Measurement Counter: Network Interface – Output Queue Length</th>
<th>NIC₅₅%</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC₅₅%</td>
<td>Maximum threshold: 30%</td>
</tr>
<tr>
<td>Indicator</td>
<td>Counter: Network Interface – Output Queue Length</td>
</tr>
<tr>
<td>Threshold: 1</td>
<td>Threshold: 1</td>
</tr>
</tbody>
</table>

NIC₅₅% = NICₚhysical * 0.03

Maximum Utilization Calculations

The highest utilization can be determined with

\[ UTIL_r = \text{MAX}(\text{CPU}_r, \text{Mem}_r, \text{Disk}_r, \text{NIC}_r) \]

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.
Diagnostic Tools

- Diagnostic Framework, on page 147
- CLI Configuration, on page 183
- Diagnostic Framework API, on page 192
- Diagnostic Framework Troubleshooting, on page 235
- DUMPLOG, on page 236
- EMSMON, on page 239

Diagnostic Framework

Overview

Unified ICM/Unified CCE/Unified CCH 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 192.

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 156.

Installation and Configuration

The Diagnostic Framework service is installed as part of the Unified ICM/Unified CCE/Unified CCH software by the ICM-CCE-CCH 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. 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 2008 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: 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 153.

Step 4: Record thumbprint of certificate in use.

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

---

3 The Unified ICM installer detects and installs the appropriate .NET version.
Step 5: In the same command window, run `DiagFwCertMgr /task:UnbindCert` command to remove certificate binding from the current port.

Step 6: Launch Notepad and open the 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 the file and quit Notepad.

Step 8: Open a 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 the output and confirm that the preceding command completed successfully.

Step 11: (Optional) Run `DiagFwCertMgr /task:ValidateCertBinding` command again to verify changes to port number binding.

Step 12: Restart the Diagnostic Framework service.

---

**What to do next**

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

**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 153.

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

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 basic 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.

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 the CONFIG domain security group of the Unified ICM/Unified CCE/Unified CCH instance being accessed: A Unified ICM/Unified CCE/Unified CCH 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/Unified CCH 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: 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 Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted 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 44: Domain Authorization Combination**

<table>
<thead>
<tr>
<th>Unified ICM Instances on Server</th>
<th>User Type</th>
<th>Instance Name Provided</th>
<th>Authorization Criteria</th>
<th>Response Content on Successful Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple</td>
<td>Domain</td>
<td>No</td>
<td>Fail authorization, user must provide instance name in request</td>
<td>HTTP 403 – Access Forbidden</td>
</tr>
<tr>
<td>Multiple</td>
<td>Domain</td>
<td>Yes</td>
<td>Authorize against the instance name provided by user</td>
<td>Data for instance requested</td>
</tr>
<tr>
<td>Multiple</td>
<td>Local</td>
<td>No</td>
<td>Authorize against local group</td>
<td>Data for all instances</td>
</tr>
</tbody>
</table>
### 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-CCH 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-CCH 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. Recall that 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 security.

When you access the service with the self signed certificate for the first time from Internet Explorer, 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.

---

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.
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>]

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>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateAndBindCert</td>
<td>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-CCE-CCH Install)</td>
</tr>
<tr>
<td>BindCertFromStore</td>
<td>Looks up the certificate provided by /certhash argument in certificate store and binds it with the HTTP service on the given port.</td>
</tr>
<tr>
<td>UnbindCert</td>
<td>Removes the certificate binding from the specified port, does not modify any certificate in the store</td>
</tr>
<tr>
<td>UnbindAndDeleteCert</td>
<td>Removes the certificate binding from the specified port. Also, deletes the self-signed certificate created by CreateAndBindCert option. (Used by ICM-CCE-CCH Uninstall)</td>
</tr>
<tr>
<td>ValidateCertBinding</td>
<td>Verifies the certificate binding on the specified port and confirms its presence in the local computer certificate store.</td>
</tr>
</tbody>
</table>
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**

Use the MMC Certificates snap-in to import a certificate in the Local Computer Personal certificate store. See the section “Import the Certificate into the Local Computer Store” of the Microsoft KB article 816794 – “HOW TO: Install Imported Certificates on a Web Server in Windows Server 2003.”

[http://support.microsoft.com/kb/816794](http://support.microsoft.com/kb/816794)

These directions apply to Windows Server 2008.

---

**Caution**

Do not follow the instructions in the “Assign the Imported Certificate to the Web Site” section of the article. 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


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-CCH Tools > Unified CLI. A new DOS Window opens with an initial prompt for your credentials (username and password).
On authentication, you can use the CLI from this window, as explained in Unified CLI Architecture, on page 157.

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 152.

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.
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 executed in system mode. User can optionally limit the system command to be executed 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 execute the system command by prefixing the “system” on any regular command. For example, “system show all” or typing “system” and executing 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 executed 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 Master 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 gets executed on a system running 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 46: CLI Commands

<table>
<thead>
<tr>
<th>Command (Verb )</th>
<th>Noun</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>all</td>
<td>Aggregation of output for all the supported nouns and specific to the verb “show.”</td>
</tr>
<tr>
<td></td>
<td>component</td>
<td>Lists the currently installed components on the server.</td>
</tr>
<tr>
<td></td>
<td>configuration</td>
<td>Lists the application configuration.</td>
</tr>
<tr>
<td></td>
<td>debug</td>
<td>Shows the current debug levels.</td>
</tr>
<tr>
<td></td>
<td>license</td>
<td>Shows the license/port information.</td>
</tr>
<tr>
<td></td>
<td>log</td>
<td>Shows the logs.</td>
</tr>
<tr>
<td></td>
<td>perf</td>
<td>Shows the performance information.</td>
</tr>
<tr>
<td></td>
<td>platform</td>
<td>Shows the platform information.</td>
</tr>
<tr>
<td></td>
<td>sessions</td>
<td>Shows the current active sessions/calls. (Not supported by Unified CCE)</td>
</tr>
<tr>
<td></td>
<td>tech-support</td>
<td>Shows system information for Tech-Support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: This command is exactly the same as “show all”.</td>
</tr>
<tr>
<td></td>
<td>trace</td>
<td>Shows the traces.</td>
</tr>
<tr>
<td></td>
<td>version</td>
<td>Shows system hardware and software status and version.</td>
</tr>
<tr>
<td></td>
<td>devices</td>
<td>Shows information of devices that are known to the CLI.</td>
</tr>
<tr>
<td>debug</td>
<td>level</td>
<td>Sets the specific debug level.</td>
</tr>
<tr>
<td>help</td>
<td>—</td>
<td>Shows the help information.</td>
</tr>
<tr>
<td>quit</td>
<td>—</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>capture</td>
<td>—</td>
<td>Captures the network packets. (Not supported by Unified CCE)</td>
</tr>
</tbody>
</table>
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.

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.

This command is used only in Unified CCE to avoid collecting OPC and VRU capture files by default.
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 regexp 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 reltime 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 normal 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**

```markdown
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**

```markdown
show license
```

**In System Mode**

```markdown
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**

```markdown
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

tool show log component cvp:callserver - displays contents of all the log files for component cvp:callserver; can be a huge output

tool 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

tool 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.

tool 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

Syntax

show perf 

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|cvp|ucm
show version server 10.86.129.11(cvp)
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 normal 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 dcomponent "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.
You can add product specific extensions; however, any extension must be reviewed by this common cross-product team for clarity and consistency.

Table 47: System Mode Syntax

<table>
<thead>
<tr>
<th>Command (Verb)</th>
<th>Noun</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td></td>
<td>Enter the interactive system mode of the CLI. Use quit/exit command to exit the system mode.</td>
</tr>
</tbody>
</table>

System Command (show all)

**Syntax**

`show all`

The system command can also be executed 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 startdatetime enddatetime] [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
Automated Command Execution

CLI or System CLI commands can be executed 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: 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 Intellengence 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, IOSGW, IOS, Location_1, cisco, cisco, 23, cisco,
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 48: Device, Protocol, and Command Mapping

<table>
<thead>
<tr>
<th>Command</th>
<th>CVP</th>
<th>Unified CCE</th>
<th>EA</th>
<th>CUIC</th>
<th>Speech Server</th>
<th>Media Server</th>
<th>Trace Server</th>
<th>IOS GW</th>
<th>Unified CM</th>
<th>Unified CCX</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture</td>
<td>REST</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
<td>REST</td>
<td>REST</td>
<td>REST</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
</tr>
<tr>
<td>config</td>
<td>REST</td>
<td>REST</td>
<td>REST</td>
<td>REST</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
<td>TELNET</td>
<td>✘</td>
<td>✘</td>
</tr>
<tr>
<td>debug</td>
<td>REST</td>
<td>REST</td>
<td>REST</td>
<td>REST</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
<td>TELNET</td>
<td>SOAP</td>
<td>REST</td>
</tr>
<tr>
<td>license</td>
<td>REST</td>
<td>REST</td>
<td>REST</td>
<td>REST</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
<td>TELNET</td>
<td>SOAP</td>
<td>REST</td>
</tr>
<tr>
<td>log</td>
<td>REST</td>
<td>REST</td>
<td>✘</td>
<td>✘</td>
<td>REST</td>
<td>REST</td>
<td>REST</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
</tr>
<tr>
<td>perf</td>
<td>REST</td>
<td>REST</td>
<td>✘</td>
<td>✘</td>
<td>REST</td>
<td>REST</td>
<td>REST</td>
<td>TELNET</td>
<td>✘</td>
<td>✘</td>
</tr>
<tr>
<td>platform</td>
<td>REST</td>
<td>REST</td>
<td>SOAP</td>
<td>SOAP</td>
<td>REST</td>
<td>REST</td>
<td>REST</td>
<td>TELNET</td>
<td>SOAP</td>
<td>SOAP</td>
</tr>
<tr>
<td>sessions</td>
<td>REST</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
<td>TELNET</td>
<td>✘</td>
<td>✘</td>
</tr>
<tr>
<td>trace</td>
<td>REST</td>
<td>REST</td>
<td>SOAP</td>
<td>SOAP</td>
<td>REST</td>
<td>✘</td>
<td>✘</td>
<td>TELNET</td>
<td>SOAP</td>
<td>SOAP REST</td>
</tr>
<tr>
<td>version</td>
<td>REST</td>
<td>REST</td>
<td>SOAP</td>
<td>REST</td>
<td>SOAP</td>
<td>REST</td>
<td>REST</td>
<td>TELNET</td>
<td>SOAP</td>
<td>SOAP REST</td>
</tr>
</tbody>
</table>

- ✘ — Not supported
- ✗ — Unknown

CLI has the master 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.

Master 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 master 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 49: Mapping of System CLI Commands to IOS CLI Commands

<table>
<thead>
<tr>
<th>System CLI</th>
<th>IOS CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>“show config”</td>
<td>“show running-config”</td>
</tr>
<tr>
<td>“show version”</td>
<td>“show version”</td>
</tr>
<tr>
<td>“show license”</td>
<td>“show license”</td>
</tr>
<tr>
<td>“show perf”</td>
<td>“show call resource voice stat”</td>
</tr>
<tr>
<td></td>
<td>“show memory statistics”</td>
</tr>
<tr>
<td></td>
<td>“show processes cpu history”</td>
</tr>
<tr>
<td></td>
<td>“show processes memory sorted”</td>
</tr>
<tr>
<td></td>
<td>“show voice dsp group all”</td>
</tr>
<tr>
<td></td>
<td>“show voice dsp voice”</td>
</tr>
<tr>
<td>“show debug”</td>
<td>“show debug”</td>
</tr>
<tr>
<td>“show log”</td>
<td>N/A</td>
</tr>
<tr>
<td>“show sessions”</td>
<td>“show call active voice compact”</td>
</tr>
<tr>
<td>“show tech-support”</td>
<td>“show tech-support”</td>
</tr>
<tr>
<td></td>
<td>&lt;Everything else given above&gt;</td>
</tr>
<tr>
<td>“show trace”</td>
<td>“show logging”</td>
</tr>
<tr>
<td>“show platform”</td>
<td>“show diag”</td>
</tr>
<tr>
<td>“debug”</td>
<td>0 no debug all</td>
</tr>
<tr>
<td></td>
<td>1 -</td>
</tr>
<tr>
<td></td>
<td>deb ccsip err</td>
</tr>
<tr>
<td></td>
<td>deb cch323 err</td>
</tr>
<tr>
<td></td>
<td>deb voip app vxml err</td>
</tr>
<tr>
<td></td>
<td>deb http client err</td>
</tr>
<tr>
<td></td>
<td>deb mrcp err</td>
</tr>
<tr>
<td></td>
<td>deb rtsp err</td>
</tr>
<tr>
<td></td>
<td>deb h225 asnl err</td>
</tr>
<tr>
<td></td>
<td>deb h245 asnl err</td>
</tr>
<tr>
<td>2 -</td>
<td>debug isdn q931</td>
</tr>
<tr>
<td></td>
<td>debug h225 events</td>
</tr>
<tr>
<td></td>
<td>debug h245 events</td>
</tr>
<tr>
<td></td>
<td>debug voip ccapi inout</td>
</tr>
<tr>
<td></td>
<td>debug vtsp events</td>
</tr>
<tr>
<td>3 -</td>
<td>debug ccsip messages</td>
</tr>
<tr>
<td></td>
<td>debug h225 q931</td>
</tr>
<tr>
<td></td>
<td>debug h225 asnl</td>
</tr>
<tr>
<td></td>
<td>debug h245 asnl</td>
</tr>
</tbody>
</table>

### 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)

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
The single API command, GetMenu, 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 GetMenu command recognizes and support machines with multiple instances [Hosted environment] installed. Because this GetMenu command is built directly into the Diagnostic Framework, no special client side files or installations are needed to access it. You can access the command from any machine with a compatible browser (for example, Internet Explorer).

The entry point for the menu utility is through the GetMenu command within the Diagnostic Framework. An example request is as follows:


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.

For Windows 2008, Unified CCE process windows no longer appear in the taskbar. This means that the user can no longer use the taskbar to view process status information, for example, whether the process is active or not. To address this, the user can view process status information and process running time in the Diagnostic Framework Portico.

The following is a sample screen:

![Figure 30: Unified ICM-CCE-CCH Diagnostic Framework Portico](image)

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 when:

- a process restarted (in the last ten minutes), uptime is underlined and highlighted in red.
- a process restarted (more than 10 minutes ago but less than 30 minutes ago) uptime is yellow.
- 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 though a browser (Internet Explorer). 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:


The IE 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 192.

The complication with this technique is that there are many APIs, and many of them contain various parameters that you must properly specify.

For downloading a Portico ListTraceFiles or GetConfigurationCategory files in Zip format using IE 9, make sure that the Do not save encrypted pages to disk option in the Security settings in the Advanced Tab of Tools > Internet Options is unchecked.

## 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

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.
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.

<table>
<thead>
<tr>
<th>Enable Serviceability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Serviceability:</td>
</tr>
<tr>
<td>Username:</td>
</tr>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>Confirm Password:</td>
</tr>
<tr>
<td>Port:</td>
</tr>
</tbody>
</table>

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**  If installing on Windows 7, ignore “Unsupported OS” warning and click **OK**.

**Step 3**  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.

---

**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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Navigate to C:\icm\serviceability\wsccli\conf.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Copy file devices-sample.csv and save as devices.csv.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Within each line you must specify the following required fields:</td>
</tr>
<tr>
<td>• IP address and hostname</td>
<td></td>
</tr>
<tr>
<td>• Device Type (from the options listed at the top of the file)</td>
<td></td>
</tr>
<tr>
<td>• Username</td>
<td></td>
</tr>
<tr>
<td>• Password</td>
<td></td>
</tr>
<tr>
<td>• Port Number (leave the default 23 in most cases)</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In addition, specifying the following fields make usage easier:</td>
</tr>
<tr>
<td>• Description</td>
<td></td>
</tr>
<tr>
<td>• Group (for example, UCCE-SideA)</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 3** | Save `devices.csv` when complete.

#### 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
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>
<thead>
<tr>
<th>Trace Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Product/component install default, should have no/minimal performance impact</td>
</tr>
<tr>
<td>1</td>
<td>Less detailed trace messages, small performance impact</td>
</tr>
<tr>
<td>2</td>
<td>More detailed trace messages, medium performance impact</td>
</tr>
<tr>
<td>3</td>
<td>If the trace level does not match any pre-defined levels (for example, a manually configured, specific trace mask), Diagnostic Framework returns “custom (99)”.</td>
</tr>
</tbody>
</table>

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

**Request:**

```
Component/Subcomponent
```

**Reply example:**
SetTraceLevel

For more information about the trace level values, see GetTraceLevel, on page 192.

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"
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.
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.

Subsequent download requests with the same filename return with an error because after the file is downloaded, it is deleted from the server.

Request:


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
<?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:


Reply example:

```xml
<?xml version="1.0" encoding="utf-8" ?>
<dp:ListLogComponentsReply ReturnCode="0" xmlns:dp="http://www.cisco.com/vtg/diagnosticportal">
<dp:Schema Version="1.0" />
<dp:LogComponentList>
<dp:LogComponent Name="ICM Installation and Upgrade" Description="ICM Installation and Upgrade logs" />
<dp:LogComponent Name="ICMDBA" Description="ICM DBA logs" />
<dp:LogComponent Name="Performance Counter" Description="Performance Counter Logs" />
<dp:LogComponent Name="Active Directory" Description="Logs for troubleshooting Active Directory issues."
```

Diagnostic Tools

Serviceability Best Practices Guide for Cisco ICM/Unified Contact Center Enterprise, Release 10.5(1)
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:


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”.

Logs" />
<dp:LogComponent Name="Cisco ICM Diagnostic CLI" Description="Cisco ICM Diagnostic CLI Logs" />
<dp:LogComponent Name="Dr Watson" Description="Dr.Watson logs" />
<dp:LogComponent Name="Cisco Security Agent" Description="Cisco Security Agent logs" />
<dp:LogComponent Name="Security Hardening" Description="Security Hardening logs" />
<dp:LogComponent Name="Web Setup" Description="Web Setup troubleshooting and audit logs" />
</dp:LogComponentList>
</dp:ListLogComponentsReply>
ListAppServers

Lists the applications and application components installed on the target server. Request:


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:


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:


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>
GetPlatformInformation

Fetches server and operating system platform details.

Request:


Reply example:

```xml
<?xml version="1.0" encoding="utf-8" ?>
<Schema Version="1.0" />
<PlatformInformation>
<PropertyList>
<Property Name="Host Name" Value="BUZZARDS-BAY" />
<Property Name="OS Platform" Value="Win32NT" />
<Property Name="OS Service Pack" Value="Service Pack 2" />
<Property Name="OS Version" Value="5.2.3790.131072" />
<Property Name="OS Version String" Value="Microsoft Windows NT 5.2.3790 Service Pack 2" />
<Property Name="System Directory" Value="C:\WINDOWS\system32" />
<Property Name="User Domain Name" Value="SILVERBACK" />
<Property Name="Common Language Runtime Version" Value="2.0.50727.3053" />
<Property Name="Admin Password Status" Value="3 []" />
<Property Name="Daylight Time In Effect" Value="True []" />
<Property Name="User Name" Value="[unavailable]" />
<Property Name="Computer Manufacturer" Value="HP" />
<Property Name="Model" Value="ProLiant DL380 G5" />
<Property Name="Number Of Processors" Value="[unavailable]" />
<Property Name="Boot Device" Value="\Device\HarddiskVolume1" />
<Property Name="Build Number" Value="3790" />
<Property Name="Build Type" Value="Multiprocessor Free" />
<Property Name="Caption" Value="Microsoft (R) Windows (R) Server 2008 R2" />
<Property Name="Current Time Zone" Value="-240" />
<Property Name="IS OS a Debug version?" Value="False" />
<Property Name="Free Physical Memory" Value="653648" />
<Property Name="Free Virtual Memory" Value="2724228" />
<Property Name="Install Date" Value="Friday, February 13, 2009 3:03:50 PM" />
<Property Name="Large System Cache" Value="1 []" />
<Property Name="Locale Code" Value="0409" />
<Property Name="Max Process Memory Size" Value="2097024" />
<Property Name="Number Of Processes" Value="66" />
<Property Name="Number Of Users" Value="10" />
<Property Name="ServicePackMajorVersion" Value="2" />
<Property Name="ServicePackMinorVersion" Value="0" />
<Property Name="System Directory" Value="C:\WINDOWS\system32" />
<Property Name="Value" Value="C:\" />
<Property Name="Total Virtual Memory" Value="4044744" />
<Property Name="Total Visible Memory" Value="2094952" />
<Property Name="Windows Directory" Value="C:\WINDOWS" />
</PropertyList>
</GetPlatformInformationReply>
```
GetNetStat

Execute a NETSTAT command remotely on the target server and return the results.

Request:

Reply:
Returns a text file with the output from the command execution.

GetIPConfig

Execute an IPCONFIG command remotely on the target server and return the results.

Request:

Reply:
Returns a text file with the output from the command execution.

GetTraceRoute

Execute 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 execution.

GetPing

Execute a PING command remotely on the target server and return the results.

Request:

Reply:
Returns a text file with the output from the command execution.

ListProcesses

Lists application processes running on the target server.

Request:
ListServices

Lists application services running on the target server.

Request:


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>
GetPerformanceInformation

Get a set of System and Application Performance Counters for the specified server.

Request:


Reply example:

<?xml version="1.0" encoding="utf-8" ?>
  <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="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:

GetAlarms

Retrieves up to 25 of the most recent alarms generated by the Unified CCE.

Request:


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="24_1_B_clgr" SubComponent="rtr" Message="Side B clgr process is OK." />
</dp:AlarmList>
</dp:GetAlarmsReply>
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_tsyr" 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_tsyr" 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="2"
Instance="acme"
Component="3_4_WACHUSETT_ICM\acme\Distributor_uaw" SubComponent="nm" Message="Process uaw on ICM\acme\Distributor node restarting process after having delayed restart for 1 seconds." />
<dp:Alarm DateTime="Jul 24, 2009 15:42:18 +0000" Type="Raise" Id="102C10F" Severity="2"
Instance="acme"
Component="3_4_WACHUSETT_ICM\acme\Distributor_uaw" SubComponent="nm" Message="Communicating with peer Synchronizer established." />
<dp:Alarm DateTime="Jul 24, 2009 15:37:55 +0000" Type="Clear" Id="1028103" Severity="1"
Instance="acme"
Component="4_1_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." />
is down after running for 30 seconds. It will restart after delaying 1 second for related operations to complete."

 dhcp: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:


Reply example:

```xml
<?xml version="1.0" encoding="utf-8" ?>
<dp:SetAlarmsReply ReturnCode="0">
</dp:SetAlarmsReply>
```

**SNMP/Syslog REST API**

The Unified CCE SNMP implementation includes a set of SNMP agents (one master and a set of subagents), and a service that manages the agent infrastructure. The SNMP master 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 master 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 Best Practices 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 51: Parameters of General Information API String Get

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>GET</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>The GET operation on the service endpoint retrieves the details of the SNMP General Information. GET https://&lt;server&gt;:&lt;port&gt;/icm-dp/rest/DiagnosticPortal/snmp/GeneralInfo</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Request Data Structure</td>
<td>In this implementation, the user sends the identifier in the request path parameter.</td>
</tr>
<tr>
<td>Response Data Structure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;?xml version=&quot;1.0&quot; encoding=&quot;utf-8&quot;?&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;dp:GeneralInformationReply ReturnCode=&quot;0&quot;&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;dp:Schema Version=&quot;1.0&quot;/&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:GeneralInformation</a></td>
</tr>
<tr>
<td></td>
<td><a href="">dp:systemName</a>user_name&lt;/dp:systemName&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:systemLocation</a>----&lt;/dp:systemLocation&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:systemContact</a>----&lt;/dp:systemContact&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:systemDescription</a>Cisco Contact Center Application Server&lt;/dp:systemDescription&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:agentPollsPort</a>1&lt;/dp:agentPollsPort&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:enableAuthenticationTraps</a>false&lt;/dp:enableAuthenticationTraps&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:agentExecutionPriority</a>1&lt;/dp:agentExecutionPriority&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:maximumConcurrentRequests</a>5&lt;/dp:maximumConcurrentRequests&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:maximumSubagentWaitTime</a>25&lt;/dp:maximumSubagentWaitTime&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:maximumSubagents</a>25&lt;/dp:maximumSubagents&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:agentLogQuantity</a>1&lt;/dp:agentLogQuantity&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/dp:GeneralInformation&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/dp:GeneralInformationReply&gt;</td>
</tr>
<tr>
<td>Response Header</td>
<td>Return 200 OK.</td>
</tr>
<tr>
<td></td>
<td>Response headers:</td>
</tr>
<tr>
<td></td>
<td>HTTP/1.1 200 OK</td>
</tr>
<tr>
<td></td>
<td>Transfer-Encoding: chunked</td>
</tr>
<tr>
<td></td>
<td>Content-Type: application/xml</td>
</tr>
<tr>
<td></td>
<td>Server: Microsoft-HTTPAPI/2.0</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>systemName</td>
<td>Represents the host name (or fully qualified domain name).</td>
<td>String</td>
<td>Length &lt;= 127</td>
<td>No</td>
<td>Alphanumeric</td>
</tr>
<tr>
<td>systemLocation</td>
<td>Represents the physical location of this host.</td>
<td>String</td>
<td>Length &lt;= 127</td>
<td>No</td>
<td>Alphanumeric</td>
</tr>
<tr>
<td>systemContact</td>
<td>Represents the name of the person to contact if a problem arises with this host.</td>
<td>String</td>
<td>Length &lt;= 127</td>
<td>No</td>
<td>Alphanumeric</td>
</tr>
<tr>
<td>systemDescription</td>
<td>Represents the Description of this host(any information deemed relevant).</td>
<td>String</td>
<td>Length &lt;= 127</td>
<td>No</td>
<td>Alphanumeric</td>
</tr>
<tr>
<td>agentPollsPort</td>
<td>Represents the port number that the SNMP Master agent listens for inbound requests.</td>
<td>String</td>
<td>Length &lt;= 5</td>
<td>No</td>
<td>Numeric</td>
</tr>
<tr>
<td>enableAuthenticationTraps</td>
<td>When enabled, sends a trap when an authentication failure occurs.</td>
<td>Boolean</td>
<td>-</td>
<td>No</td>
<td>true /false; case sensitive</td>
</tr>
<tr>
<td>agentExecutionPriority</td>
<td>Represents the thread execution priority for all SNMP agents.</td>
<td>Int</td>
<td>0-2</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>maximumConcurrentRequests</td>
<td>Represents the maximum concurrent SNMP Objects request that are allowed.</td>
<td>Unsigned Int</td>
<td>2-32</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>maximumSubagentWaitTime</td>
<td>Represents the maximum number of seconds a master agent will wait for a subagent to respond to a request (timeout).</td>
<td>Unsigned Int</td>
<td>5-150</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>maximumSubagents</td>
<td>Represents the maximum number of SNMP subagents the master agent permits to be loaded.</td>
<td>Unsigned Int</td>
<td>5-150</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>agentLogQuantity</td>
<td>Represents the number of log messages to be written to the agent log files.</td>
<td>Int</td>
<td>0-2</td>
<td>No</td>
<td>-</td>
</tr>
</tbody>
</table>
Update

This implementation of the SNMP GeneralInfo string updates the properties of the General Information API.

Table 52: Parameters of General Information API String Update

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>PUT</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>The PUT operation on the service endpoint updates the properties of the General Information API.</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Request Data Structure</td>
<td><code>&lt;GeneralInformation&gt;</code></td>
</tr>
<tr>
<td>Response Header</td>
<td>Return 200 OK.</td>
</tr>
<tr>
<td>Response Code</td>
<td>400- Bad request. If the request body is invalid.</td>
</tr>
<tr>
<td></td>
<td>400- API error. If the object either does not exist or is stale.</td>
</tr>
<tr>
<td></td>
<td>403- Authorization Failure (for example, the user is not authenticated in the web session).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>503 Service Unavailable. When the request processing threshold is reached.</td>
</tr>
<tr>
<td>Security Constraints</td>
<td>Only a Serviceability administrator can perform this operation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>systemName</td>
<td>Represents the host name (or fully qualified domain name).</td>
<td>String</td>
<td>Length &lt;= 127</td>
<td>No</td>
<td>Alphanumeric</td>
</tr>
<tr>
<td>Tag</td>
<td>Description</td>
<td>Data Type</td>
<td>Input Constraints</td>
<td>Required Fields</td>
<td>Possible Value</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>-------------------</td>
<td>-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>systemLocation</td>
<td>Represents the physical location of this host.</td>
<td>String</td>
<td>Length &lt;= 127</td>
<td>No</td>
<td>Alphanumeric</td>
</tr>
<tr>
<td>systemContact</td>
<td>Represents the name of the person to contact if a problem arises with this host.</td>
<td>String</td>
<td>Length &lt;= 127</td>
<td>No</td>
<td>Alphanumeric</td>
</tr>
<tr>
<td>systemDescription</td>
<td>Represents the Description of this host(any information deemed relevant).</td>
<td>String</td>
<td>Length &lt;= 127</td>
<td>No</td>
<td>Alphanumeric</td>
</tr>
<tr>
<td>agentPollsPort</td>
<td>Represents the port number that the SNMP Master agent listens for inbound requests.</td>
<td>String</td>
<td>Length &lt;= 5</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>enableAuthenticationTraps</td>
<td>When enabled, sends a trap when an authentication failure occurs.</td>
<td>Boolean</td>
<td>-</td>
<td>No</td>
<td>true/false; case sensitive</td>
</tr>
<tr>
<td>agentExecutionPriority</td>
<td>Represents the thread execution priority for all SNMP agents.</td>
<td>Int</td>
<td>0-2</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>maximumConcurrentRequests</td>
<td>Represents the maximum concurrent SNMP Objects request that are allowed.</td>
<td>Unsigned Int</td>
<td>2-32</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>maximumSubagentWaitTime</td>
<td>Represents the maximum number of seconds a master agent will wait for a subagent to respond to a request (timeout).</td>
<td>Unsigned Int</td>
<td>5-150</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>maximumSubagents</td>
<td>Represents the maximum number of SNMP subagents the master agent permits to be loaded.</td>
<td>Unsigned Int</td>
<td>5-150</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>agentLogQuantity</td>
<td>Represents the number of log messages to be written to the agent log files.</td>
<td>Int</td>
<td>0-2</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**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 53: Parameters of SNMP v1/v2c Community String Create

| HTTP Method | POST |
| Input/Output Format | XML |
| Request | The POST operation on the service endpoint creates the 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 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. |

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
<th>Additional Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Represents the community string name</td>
<td>String</td>
<td>Length &lt;= 40</td>
<td>Yes</td>
<td>Alphanumeric</td>
<td>Alphanumeric dot, underscore, and hyphens are allowed. Space is not allowed.</td>
</tr>
</tbody>
</table>
### Table 54: Parameters of SNMP v1/v2c Community String Delete

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
<th>Additional Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmpversion</td>
<td>Represents the SNMP version information</td>
<td>String</td>
<td>-</td>
<td>No</td>
<td>V1 (default), V2c</td>
<td>Only V1 or V2c; Not case sensitive.</td>
</tr>
<tr>
<td>hosts</td>
<td>Represents a list of &quot;host&quot; tags</td>
<td>-</td>
<td>-</td>
<td>No</td>
<td>If this tag is specified, then the host tag is mandatory.</td>
<td>-</td>
</tr>
<tr>
<td>host</td>
<td>Represents the management station host IP address. If the management station</td>
<td>String</td>
<td>Valid IP address; number of host tags must be &lt;= 255</td>
<td>No</td>
<td>A valid ip4 address</td>
<td>-</td>
</tr>
<tr>
<td>accessprivilege</td>
<td>Represents the access privileges of the community string.</td>
<td>String</td>
<td>-</td>
<td>No</td>
<td>ReadOnly (default), ReadWrite</td>
<td>Only ReadOnly or ReadWrite; Not case sensitive.</td>
</tr>
</tbody>
</table>

#### Delete

This implementation of SNMP v1/v2c community string deletes the community from the listed devices.

**Delete**

The DELETE operation on the service endpoint deletes the SNMP Community.

DELETE

https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/community/Name/<name>&SnmpVersion/<snmpversion>

**Response Header**

Return 200 OK.

Response headers:

HTTP/1.1 200 OK
Transfer-Encoding: chunked
Content-Type: application/xml
Server: Microsoft-HTTPAPI/2.0
<table>
<thead>
<tr>
<th>Response Code</th>
<th>400- Bad request. If the request body is invalid.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>400- API error. If the object either does not exist or is stale.</td>
</tr>
<tr>
<td></td>
<td>403- Authorization Failure (for example, the user is not authenticated in the web session).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>503 Service Unavailable. When the request processing threshold is reached.</td>
</tr>
</tbody>
</table>

| 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 55: Parameters of SNMP v1/v2c Community String Get

<table>
<thead>
<tr>
<th>URL</th>
<th>GET</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>https://&lt;server&gt;:&lt;port&gt;/icm-dp/rest/DiagnosticPortal/snmp/community/Name/&lt;name&gt;&amp;SnmpVersion/&lt;snmpversion&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>GET</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Input/Output Format</th>
<th>XML</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Request</th>
<th>The GET operation on the service endpoint retrieves the details of the SNMP community.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GET</td>
</tr>
<tr>
<td></td>
<td>https://&lt;server&gt;:&lt;port&gt;/icm-dp/rest/DiagnosticPortal/snmp/community/Name/&lt;name&gt;&amp;SnmpVersion/&lt;snmpversion&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content-type</th>
<th>Application/XML</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Request Data Structure</th>
<th>In this implementation, the user sends the identifier in the request path parameter.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;?xml version=&quot;1.0&quot; encoding=&quot;utf-8&quot;?&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;dp:CommunityReply ReturnCode=&quot;0&quot; xmlns:dp=&quot;<a href="http://www.cisco.com/vtg/diagnosticportal%22%3E">http://www.cisco.com/vtg/diagnosticportal&quot;&gt;</a></td>
</tr>
<tr>
<td></td>
<td>&lt;dp:Schema Version=&quot;1.0&quot; /&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:community</a></td>
</tr>
<tr>
<td></td>
<td><a href="">dp:name</a>str1&lt;/dp:name&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:snmpversion</a>V2c&lt;/dp:snmpversion&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:accessprivilege</a>ReadOnly&lt;/dp:accessprivilege&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:hosts</a></td>
</tr>
<tr>
<td></td>
<td><a href="">dp:host</a>192.0.2.0&lt;/dp:host&gt;</td>
</tr>
<tr>
<td></td>
<td><a href="">dp:host</a>192.0.2.1&lt;/dp:host&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/dp:hosts&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/dp:community&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;/dp:CommunityReply&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response Data Structure</th>
<th>Return 200 OK.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Response headers:</td>
</tr>
<tr>
<td></td>
<td>HTTP/1.1 200 OK</td>
</tr>
<tr>
<td></td>
<td>Transfer-Encoding: chunked</td>
</tr>
<tr>
<td></td>
<td>Content-Type: application/xml</td>
</tr>
<tr>
<td></td>
<td>Server: Microsoft-HTTPAPI/2.0</td>
</tr>
</tbody>
</table>
## SNMP v1/v2c Community

**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.

**List**
This implementation of SNMP v1/v2c community string lists all the communities that are configured on the system.

### Table 56: Parameters of SNMP v1/v2c Community String List

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>GET</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>The GET operation on the service endpoint lists the details of the SNMP community. GET https://&lt;server&gt;:&lt;port&gt;/icm-dp/rest/DiagnosticPortal/snmp/community</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
</tbody>
</table>
| Response Data Structure | `<?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>` |
| 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.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
<th>Additional Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Represents the community string name</td>
<td>String</td>
<td>Length &lt;= 40</td>
<td>Yes</td>
<td>Alphanumeric</td>
<td>Alphanumeric dot, underscore, and hyphens are allowed. Space is not allowed.</td>
</tr>
<tr>
<td>snmpversion</td>
<td>Represents the SNMP version information</td>
<td>String</td>
<td>-</td>
<td>No</td>
<td>V1 (default), V2c</td>
<td>Only V1 or V2c; Not case sensitive.</td>
</tr>
</tbody>
</table>

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 234.

Table 57: Parameters of SNMP v1/v2c Community String Update

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>PUT</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>The PUT operation on the service endpoint updates the properties of the SNMP community. PUT https://&lt;server&gt;:&lt;port&gt;/icm-dp/rest/DiagnosticPortal/snmp/community</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
</tbody>
</table>
| 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 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.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
<th>Additional Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Represents the community string name</td>
<td>String</td>
<td>Length &lt;= 40</td>
<td>Yes</td>
<td>Alphanumeric</td>
<td>Alphanumeric dot, underscore, and hyphens are allowed. Space is not allowed.</td>
</tr>
<tr>
<td>snmpversion</td>
<td>Represents the SNMP version information</td>
<td>String</td>
<td>-</td>
<td>Yes</td>
<td>V1 (default), V2c</td>
<td>Only V1 or V2c; Not case sensitive.</td>
</tr>
<tr>
<td>hosts</td>
<td>Represents a list of &quot;host&quot; tags</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>If this tag is specified, then the host tag is mandatory.</td>
<td>-</td>
</tr>
<tr>
<td>host</td>
<td>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.</td>
<td>String</td>
<td>Valid IP address; number of host tags must be &lt;= 255</td>
<td>Yes</td>
<td>A valid ip4 address</td>
<td>-</td>
</tr>
<tr>
<td>accessprivilege</td>
<td>Represents the access privileges of the community string.</td>
<td>String</td>
<td>-</td>
<td>Yes</td>
<td>ReadOnly (default), ReadWrite</td>
<td>Only ReadOnly or ReadWrite; Not case sensitive.</td>
</tr>
</tbody>
</table>

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 58: Parameters of SNMP User String Create

| HTTP Method | POST |
| Input/Output Format | XML |
| Request | The POST operation on the service endpoint creates the SNMP User. |
| Request Data Structure | POST https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/user |
| Content-type | Application/XML |
| Accept | Application/XML |

Request Data Structure

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<user>
  <name>Snmp_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>
```

Response Header

Return 201 CREATED.

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.
<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
<th>Additional Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Represents the user string name.</td>
<td>String</td>
<td>Length &lt;= 40</td>
<td>Yes</td>
<td>Alphanumeric</td>
<td>Alphanumeric dot, underscore, and hyphens are allowed. Space is not allowed.</td>
</tr>
<tr>
<td>accessprivilege</td>
<td>Represents the access privileges of the user string.</td>
<td>String</td>
<td>-</td>
<td>No</td>
<td>ReadOnly (default), ReadWrite</td>
<td>Only ReadOnly or ReadWrite; Not case sensitive.</td>
</tr>
<tr>
<td>hosts</td>
<td>Represents a list of &quot;host&quot; tags.</td>
<td>-</td>
<td>-</td>
<td>No</td>
<td>If this tag is specified, then the host tag is mandatory.</td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>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.</td>
<td>String</td>
<td>Valid IP address; number of host tags must be &lt;= 255</td>
<td>No</td>
<td>A valid ip4 address</td>
<td>-</td>
</tr>
<tr>
<td>authInfoReqd</td>
<td>Authentication information is required.</td>
<td>Boolean</td>
<td>-</td>
<td>No</td>
<td>false, true</td>
<td>Case sensitive.</td>
</tr>
<tr>
<td>authProtocol</td>
<td>Authentication protocol.</td>
<td>String</td>
<td>-</td>
<td>No</td>
<td>MD5, SHA-1</td>
<td>Value for this tag is set only when authInfoReqd is true.</td>
</tr>
<tr>
<td>authPassword</td>
<td>Authentication password.</td>
<td>String</td>
<td>-</td>
<td>No</td>
<td>Alphanumeric with any special character.</td>
<td>Value for this tag is set only when authInfoReqd is true.</td>
</tr>
<tr>
<td>Tag</td>
<td>Description</td>
<td>Data Type</td>
<td>Input Constraints</td>
<td>Required Fields</td>
<td>Possible Value</td>
<td>Additional Validation</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------</td>
<td>-----------</td>
<td>-------------------</td>
<td>-----------------</td>
<td>----------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>privacyInfoReqd</td>
<td>Privacy information is required.</td>
<td>Boolean</td>
<td>-</td>
<td>No.</td>
<td>false, true</td>
<td>Case sensitive. If privacyInfoReqd is true, then authInfoReqd must be set to true.</td>
</tr>
<tr>
<td>privacyProtocol</td>
<td>Privacy protocol.</td>
<td>String</td>
<td>-</td>
<td>No.</td>
<td>3DES AES-192 AES-256</td>
<td>Value for this tag is set only when privacyInfoReqd is true.</td>
</tr>
<tr>
<td>privacyPassword</td>
<td>Privacy password.</td>
<td>String</td>
<td>-</td>
<td>No.</td>
<td>Alphanumeric with any special character.</td>
<td>Value for this tag is set only when privacyInfoReqd is true.</td>
</tr>
</tbody>
</table>

**Delete**

This implementation of SNMP user string deletes the user from the listed devices.

**Table 59: Parameters of SNMP User String Delete**

<table>
<thead>
<tr>
<th>URL</th>
<th>DELETE https://&lt;server&gt;:&lt;port&gt;/icm-dp/rest/DiagnosticPortal/snmp/user/Name/&lt;name&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>DELETE</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>The DELETE operation on the service endpoint deletes the SNMP User.</td>
</tr>
<tr>
<td></td>
<td>DELETE https://&lt;server&gt;:&lt;port&gt;/icm-dp/rest/DiagnosticPortal/snmp/user/Name/&lt;name&gt;</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Request Data Structure</td>
<td>In this implementation, the user sends the identifier in the request path parameter.</td>
</tr>
<tr>
<td>Response Header</td>
<td>Return 200 OK.</td>
</tr>
<tr>
<td></td>
<td>Response headers: HTTP/1.1 200 OK</td>
</tr>
<tr>
<td></td>
<td>Transfer-Encoding: chunked</td>
</tr>
<tr>
<td></td>
<td>Content-Type: application/xml</td>
</tr>
<tr>
<td></td>
<td>Server: Microsoft-HTTPAPI/2.0</td>
</tr>
</tbody>
</table>
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 the SNMP user string retrieves the details of the user.

Table 60: 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 | The GET operation on the service endpoint retrieves the details of the SNMP User. |
| 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 | &lt;dp:UserReply ReturnCode="0"><br>
   &lt;dp:Schema Version="1.0"&gt;
   &lt;dp:user&gt;
     &lt;dp:name&gt;Snmp_User&lt;/dp:name&gt;
     &lt;dp:accessprivilige&gt;ReadOnly&lt;/dp:accessprivilige&gt;
     &lt;dp:host&gt;192.0.2.0&lt;/dp:host&gt;
   &lt;/dp:user&gt;
   &lt;dp:host&gt;192.0.2.0&lt;/dp:host&gt;
&lt;/dp:host&gt;
   &lt;dp:authProtoco&gt;MD5&lt;/dp:authProtoco&gt;
   &lt;dp:privacyProtoco&gt;AES-128&lt;/dp:privacyProtoco&gt;
&lt;/dp:UserReply&gt; |
| 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.

---

### List

This implementation of SNMP User string lists all the users that are configured on the system.

#### Table 61: Parameters of SNMP User String List

<table>
<thead>
<tr>
<th>URL</th>
<th>GET https://&lt;server&gt;:&lt;port&gt;/icm-dp/rest/DiagnosticPortal/snmp/user</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>GET</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>The GET operation on the service endpoint lists the details of the SNMP User.</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
</tbody>
</table>
| Response Data Structure | `<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>` |
| Response Header | Return 200 OK. |
| Response Code | 400- Bad request. If the request body is invalid. |
| Security Constraints | Only a Serviceability administrator can perform this operation. |
### SNMPv3 User

**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 234.

#### Table 62: Parameters of SNMP User String Update

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
<th>Additional Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Represents the user string name.</td>
<td>String</td>
<td>Length &lt;= 40</td>
<td>Yes</td>
<td>Alphanumeric</td>
<td>Alphanumeric dot, underscore, and hyphens are allowed. Space is not allowed.</td>
</tr>
</tbody>
</table>

**URL**

`https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/user`

**HTTP Method**

PUT

**Input/Output Format**

XML

**Request**

The PUT operation on the service endpoint updates the properties of the SNMP community.

PUT `https://<server>:<port>/icm-dp/rest/DiagnosticPortal/snmp/user`

**Content-type**

Application/XML

**Accept**

Application/XML

**Request Data Structure**

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<user>
  <name>Snmp_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>
```

**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.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
<th>Additional Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Represents the user string name.</td>
<td>String</td>
<td>Length &lt;= 40</td>
<td>Yes</td>
<td>Alphanumeric</td>
<td>Alphanumeric dot, underscore, and hyphens are allowed. Space is not allowed.</td>
</tr>
<tr>
<td>accessprivilege</td>
<td>Represents the access privileges of the user string.</td>
<td>String</td>
<td>-</td>
<td>Yes</td>
<td>ReadOnly (default), ReadWrite</td>
<td>Only ReadOnly or ReadWrite; Not case sensitive.</td>
</tr>
<tr>
<td>hosts</td>
<td>Represents a list of &quot;host&quot; tags.</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>If this tag is specified, then the host tag is mandatory.</td>
<td>-</td>
</tr>
<tr>
<td>host</td>
<td>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.</td>
<td>String</td>
<td>Valid IP address; number of host tags must be &lt;= 255</td>
<td>Yes</td>
<td>A valid ip4 address</td>
<td>-</td>
</tr>
<tr>
<td>authInfoReqd</td>
<td>Authentication information is required.</td>
<td>Boolean</td>
<td>-</td>
<td>Yes</td>
<td>false, true</td>
<td>Case sensitive.</td>
</tr>
<tr>
<td>authProtocol</td>
<td>Authentication protocol.</td>
<td>String</td>
<td>-</td>
<td>No.</td>
<td>If authInfoReqd is true, then this field is mandatory.</td>
<td>MD5SHA-1</td>
</tr>
<tr>
<td>authPassword</td>
<td>Authentication password.</td>
<td>String</td>
<td>-</td>
<td>No.</td>
<td>If authInfoReqd is true, then this field is mandatory.</td>
<td>Alphanumeric with any special character.</td>
</tr>
</tbody>
</table>
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 63: Parameters of SNMP Trap string Post

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>POST</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>POST operation on the service endpoint creates an SNMP Trap.</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
</tbody>
</table>
Request Data Structure

```
<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>
```

Response Header
Return 201 CREATED.
Response headers:
HTTP/1.1 201 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.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
<th>Additional Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Represents the trap string name.</td>
<td>String</td>
<td>Length &lt;= 41</td>
<td>Yes</td>
<td>Alphanumeric</td>
<td>Alphanumeric dot, underscore, and hyphens are allowed; Space is not allowed.</td>
</tr>
<tr>
<td>snmpversion</td>
<td>Represents the SNMP version.</td>
<td>String</td>
<td>-</td>
<td>Yes</td>
<td>V1, V2C, V3</td>
<td>V1, V2C, V3</td>
</tr>
<tr>
<td>communityOrUserRef</td>
<td>Represents a community or user for which this trap is configured.</td>
<td>String</td>
<td>Length &lt;= 41</td>
<td>Yes</td>
<td>Alphanumeric</td>
<td>Alphanumeric dot, underscore, and hyphens are allowed; Space is not allowed.</td>
</tr>
<tr>
<td>destinations</td>
<td>Represents the list of destination tag.</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>destination</td>
<td>Each destination tag has a mandatory ipAddr and port tag.</td>
<td>-</td>
<td>Number of destination tags must be &lt;= 255</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
### Table 64: Parameters of SNMP Trap string Delete

<table>
<thead>
<tr>
<th>URL</th>
<th>DELETE https://&lt;server&gt;:&lt;port&gt;/icm-dp/rest/DiagnosticPortal/snmp/trap/Name/&lt;name&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>DELETE</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>The DELETE operation on the service endpoint deletes the properties of the Traps API.</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Response Header</td>
<td>Return 200 OK.</td>
</tr>
<tr>
<td>Response Code</td>
<td>400- Bad request. If the request body is invalid.</td>
</tr>
<tr>
<td></td>
<td>400- API error. If the object either does not exist or is stale.</td>
</tr>
<tr>
<td></td>
<td>403- Authorization Failure (for example, the user is not authenticated in the web session).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>503 Service Unavailable. When the request processing threshold is reached.</td>
</tr>
<tr>
<td>Security Constraints</td>
<td>Only a Serviceability administrator can perform this operation.</td>
</tr>
</tbody>
</table>

### Delete

This implementation of SNMP Trap string deletes the traps from the listed traps.

**Table 64: Parameters of SNMP Trap string Delete**

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
<th>Additional Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipAddr</td>
<td>Represents the destination IP where traps have to be sent.</td>
<td>String</td>
<td>Valid IP address</td>
<td>Yes</td>
<td>Valid IP address</td>
<td>-</td>
</tr>
<tr>
<td>port</td>
<td>Represents the port on the destination where the traps have to be sent.</td>
<td>String</td>
<td>Length &lt;= 5</td>
<td>Yes</td>
<td>The default value 162 is assumed when:</td>
<td>Numeric.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- no value is specified</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- the value specified is 0</td>
<td></td>
</tr>
</tbody>
</table>
Get

This implementation of SNMP Trap string retrieves the details of the trap.

Table 65: Parameters of SNMP Trap string Get

<table>
<thead>
<tr>
<th>URL</th>
<th>https://&lt;server&gt;:&lt;port&gt;/icm-dp/rest/DiagnosticPortal/snmp/trap/Name/&lt;name&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>GET</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>The GET operation on the service endpoint retrieves the details of the Trap API.</td>
</tr>
<tr>
<td>GET</td>
<td>https://&lt;server&gt;:&lt;port&gt;/icm-dp/rest/DiagnosticPortal/snmp/trap/Name/&lt;name&gt;</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
</tbody>
</table>
| Response Data Structure | <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> |
| 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 66: Parameters of SNMP Trap string Get

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>GET</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>The GET operation on the service endpoint lists all the traps that are configured on the system.</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Response Header</td>
<td>Return 200 OK.</td>
</tr>
<tr>
<td>Response Code</td>
<td>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.</td>
</tr>
<tr>
<td>Security Constraints</td>
<td>Only a Serviceability administrator can perform this operation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
<th>Additional Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Represents the trap string name.</td>
<td>String</td>
<td>Length &lt;= 41</td>
<td>Yes</td>
<td>Alphanumeric</td>
<td>Alphanumeric, dot, underscore, and hyphens are allowed.</td>
</tr>
</tbody>
</table>

**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 234.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>PUT</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>The PUT operation on the service endpoint updates the properties of the SNMP trap that is mentioned in the request. PUT https://&lt;server&gt;:&lt;port&gt;/icm-dp/rest/DiagnosticPortal/snmp/trap</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
</tbody>
</table>
| Request Data Structure | <?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> |
| 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. |
<p>| Security Constraints | Only a Serviceability administrator can perform this operation. |</p>
<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
<th>Additional Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Represents the trap string name.</td>
<td>String</td>
<td>Length &lt;= 41</td>
<td>Yes</td>
<td>Alphanumeric</td>
<td>Alphanumeric dot, underscore, and hyphens are allowed.</td>
</tr>
<tr>
<td>snmpversion</td>
<td>Represents the SNMP version.</td>
<td>String</td>
<td>-</td>
<td>Yes</td>
<td>V1, V2C, V3</td>
<td>V1, V2C, V3</td>
</tr>
<tr>
<td>communityOrUserRef</td>
<td>Represents a community or user for which this trap is configured.</td>
<td>String</td>
<td>Length &lt;= 41</td>
<td>Yes</td>
<td>Alphanumeric</td>
<td>Alphanumeric dot, underscore, and hyphens are allowed.</td>
</tr>
<tr>
<td>destinations</td>
<td>Represents the list of destination tag.</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>destination</td>
<td>Each destination tag has a mandatory ipAdder and port tag.</td>
<td>-</td>
<td>Number of destination tags must be &lt;= 255</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>ipAddr</td>
<td>Represents the destination IP where traps have to be sent.</td>
<td>String</td>
<td>Valid IP address</td>
<td>Yes</td>
<td>Valid IP address</td>
<td>-</td>
</tr>
<tr>
<td>port</td>
<td>Represents the port on the destination where the traps have to be sent.</td>
<td>String</td>
<td>Length &lt;= 5</td>
<td>Yes</td>
<td>The default value 162 is assumed when:</td>
<td>Numeric.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- no value is specified</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- the value specified is 0</td>
<td></td>
</tr>
</tbody>
</table>

### 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 234.
### Table 68: Parameters of syslog API String Create

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>PUT</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>The PUT operation on the service endpoint updates the details of the SNMP REST syslog API.</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
</tbody>
</table>
| Request Data Structure | ```xml
<?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>
``` |
| Response Header | Return 200 OK. |
| 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. |
## Additional Validation Possible Value Required Fields

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Data Type</th>
<th>Input Constraints</th>
<th>Required Fields</th>
<th>Possible Value</th>
<th>Additional Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>loggerNode</td>
<td>Represents the logger node.</td>
<td>String</td>
<td>-</td>
<td>Yes</td>
<td>LoggerA or LoggerB</td>
<td>Only LoggerA or LoggerB; Not case sensitive</td>
</tr>
<tr>
<td>enableFeed</td>
<td>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.</td>
<td>Boolean</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>true/false; case sensitive.</td>
</tr>
<tr>
<td>collectorAddressList</td>
<td>Represents a list of collectorAddress.</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>collectorAddress</td>
<td>Each collectorAddress tag should have a mandatory address and port tag.</td>
<td>-</td>
<td>Number of collectorAddress tags must be &lt;= 5</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>address</td>
<td>Represents the Syslog collector IP address or host name.</td>
<td>String</td>
<td>Host or IP address</td>
<td>Yes</td>
<td>Alphanumeric</td>
<td>A valid host name or IP address.</td>
</tr>
<tr>
<td>port</td>
<td>Port on the syslog collector destination.</td>
<td>String</td>
<td>Value should be &lt;= 65535</td>
<td>Yes</td>
<td>Only numeric</td>
<td>514 (default). If value is specified as 0, then the default value is assumed.</td>
</tr>
<tr>
<td>disablePing</td>
<td>If set to true, disables ping messages to the syslog collector destination.</td>
<td>Boolean</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
<td>true/false; case sensitive.</td>
</tr>
</tbody>
</table>

### List
This implementation of syslog lists all the instances that are configured on the system.

*Table 69: Parameters of Syslog API String List*

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>GET</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>The GET operation on the service endpoint lists the instances of the SNMP REST syslog API that are configured on the system.</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
</tbody>
</table>
Response Data Structure

```xml
<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>
```

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.

Get

This implementation of syslog retrieves the details of the syslog parameters for a logger instance.

Table 70: Parameters of Syslog API String

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>GET</td>
</tr>
<tr>
<td>Input/Output Format</td>
<td>XML</td>
</tr>
<tr>
<td>Request</td>
<td>The GET operation on the service endpoint retrieves the details of the syslog parameters for a logger instance.</td>
</tr>
<tr>
<td></td>
<td>GET https://&lt;server&gt;:&lt;port&gt;/icm-dp/rest/DiagnosticPortal/syslog/syslogInstanceName/&lt;name&gt;&amp;loggerNode/&lt;node&gt;</td>
</tr>
<tr>
<td>Content-type</td>
<td>Application/XML</td>
</tr>
<tr>
<td>Accept</td>
<td>Application/XML</td>
</tr>
</tbody>
</table>
### 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:

```
<?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:

```
<?xml version="1.0" encoding="utf-8"?>
<community>
  <name>Public_Community</name>
</community>
```
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>
<thead>
<tr>
<th>Issue</th>
<th>Troubleshooting / Remedy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnostic Framework service does not start</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Make sure none of the configuration files is missing.</td>
</tr>
<tr>
<td></td>
<td>Check Event Viewer and Diagnostic Framework log file for any initialization errors.</td>
</tr>
<tr>
<td>Cannot access any API from the supported browser client</td>
<td>Confirm that you are using a supported browser by checking the Compatibility Matrix for Unified CCE at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html</a>.</td>
</tr>
<tr>
<td></td>
<td>Confirm the base URL is correct; compare it with the URL in the service configuration file DiagFwSvc.exe.config.</td>
</tr>
<tr>
<td></td>
<td>Confirm the API used is valid; try accessing the built GetMenu API.</td>
</tr>
<tr>
<td></td>
<td>Make sure the API is accessed using HTTPS.</td>
</tr>
<tr>
<td></td>
<td>Make sure the credentials used as valid, check Windows Event log for any authentication errors and Diagnostic Framework log for any authorization errors.</td>
</tr>
<tr>
<td></td>
<td>Use DiagFwCertMgr utility to validate the certificate binding to the port in use. Recreate or rebind the certificate if any issues were found.</td>
</tr>
<tr>
<td></td>
<td>Clear the supported browser cache and restart the browser.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Use DiagFwCertMgr utility to validate the certificate binding to the port in use. Recreate or rebind the certificate if any issues were found.</td>
</tr>
</tbody>
</table>
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/prodtech_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.

Note

The contents of the APPNAME and TAGS fields differ from those previously described in section 5.1.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPNAME</td>
<td>PRODUCT_COMPONENT_MESSAGECATEGORY</td>
</tr>
<tr>
<td></td>
<td>PRODUCT - always ICM</td>
</tr>
<tr>
<td></td>
<td>COMPONENT – such as Router</td>
</tr>
<tr>
<td></td>
<td>MESSAGECATEGORY – such as ProcessSynchronization</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>TAGS</td>
<td>Acceptable tags are:</td>
</tr>
<tr>
<td></td>
<td>[comp=%s] - component name including side, such as Router A</td>
</tr>
<tr>
<td></td>
<td>[pname=%s] - process name, such as rtr</td>
</tr>
<tr>
<td></td>
<td>[iid=%s] - instance name, such as acme</td>
</tr>
<tr>
<td></td>
<td>[sev=%s] – severity, such as info</td>
</tr>
<tr>
<td></td>
<td>and optionally [part=%%1.%%2.%%3], which is used only for multi-line entries as described later in this section.</td>
</tr>
</tbody>
</table>

**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:
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
```
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.


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> [... ] <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**
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

A single EMSMON can monitor multiple processes and merge their output (for example, [jgw1 and pim1]). Use one EMSMON only for each process.

Run EMSMON Remotely

To reserve system resources for Unified CCE processes, run the EMSMON client on a remote machine that does not host Unified CCE processes. For example, do not run the EMSMON client on side A of a PG and connect it to a process on side B of a PG.

Procedure

Copy emsmon.exe, emsmon.pdb, and icrmessages.dll from c:\icm\bin and place files on remote machine.

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.

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.
MIB Results Example Appendix

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 =
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)
Serviceability Best Practices Guide for Cisco ICM/Unified Contact Center Enterprise, Release 10.5(1)
cccaRouterDuplexPairName.0.1 = cc-rgr1a
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-rgr1a
cccaLoggerRouterSideBName.0.2 = cc-rgr1a
cccaLoggerDuplexPairName.0.2 = cc-rgr1a
cccaLoggerHDSReplication.0.2 = 0
cccaDistAwSide.0.4 = sideA(1)
cccaDistAwType.0.4 = standard(0)
cccaDistAwAdminSiteName.0.4 = cc-rgr1a
cccaDistAwRouterSideAName.0.4 = cc-rgr1a
cccaDistAwRouterSideBName.0.4 = cc-rgr1a
cccaDistAwLoggerSideAName.0.4 = cc-rgr1a
cccaDistAwLoggerSideBName.0.4 = cc-rgr1a
cccaDistAwDuplexPairName.0.4 = cc-rgr1a
cccaDistAwHDSEnabled.0.4 = 0
cccaDistAwWebViewEnabled.0.4 = false(2)
cccaPgNumber.0.3 = 1
cccaPgSide.0.3 = sideA(1)
cccaPgRouterSideAName.0.3 = cc-rgr1a
cccaPgRouterSideBName.0.3 = cc-rgr1a
cccaPgDuplexPairName.0.3 = cc-rgr1a
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
SNMP Notifications Reference

- Unified ICM/Unified CCE SNMP Notifications, on page 245
- Node Manager Events, on page 246
- Message Delivery Events, on page 252
- Router Events, on page 258
- Logger Events, on page 265
- Peripheral Gateway (PG) Events, on page 270
- Administrator Workstation Events, on page 283
- Outbound Option Events, on page 283
- ICM Network Interface Controller (NIC) Events, on page 294
- ICM Hosted Events, on page 349
- Symposium/AAS Events, on page 352
- Live Data Events (Packaged CCE only), on page 362

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.
## Node Manager Events

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1028101</td>
<td>Message</td>
<td>%1 Node Manager initializing.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The node management library, common to nearly all ICM processes, is initializing itself. This is standard practice when a process (re)starts.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1028103</td>
<td>Message</td>
<td>%1 Node Manager started. Last shutdown was by operator request.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Node Manager successfully started. The last reason the Node Manager stopped was because a clean shutdown of the ICM node was requested by the operator.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1028104</td>
<td>Message</td>
<td>%1 Node Manager started. Last shutdown was due to system shutdown.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1028105</td>
<td>Message</td>
<td>The operator/administrator has shutdown the ICM software on %1.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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', 'net stop', Control Panel Services, or shuts down the node.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the operator/administrator to determine the reason for the shutdown.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1029101</td>
<td>Message</td>
<td>%1 Node Manager Manager started.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Node Manager Manager process (which oversees the Node Manager process) has started.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>102C101</td>
<td>Message</td>
<td>%1 node critical process %2 died. Rebooting node.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A critical process needed to run the ICM software on this node has died. The Node Manager is forcing a reboot of the node.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>102C103</td>
<td>Message</td>
<td>%1 node restarting process %2.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Node Manager is restarting process %2 after the process died or was terminated.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>102C107</td>
<td>Message</td>
<td>%1 Node Manager started. Last shutdown was for reboot after failure of critical process.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Node Manager has started. The last shutdown was requested by the Node Manager since it recognized that a critical process for the node failed.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>102C108</td>
<td>Message</td>
<td>%1 Node Manager started. Last shutdown was for unknown reasons. Possible causes include a power failure, a system failure or a Node Manager exit.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Node Manager has started. The Node Manager cannot determine why the system is restarting. Possible causes are: power failure, a system failure (Windows NT blue screen), a system not responding (in which an operator forced a reboot), or the Node Manager exit.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>102C109</td>
<td>Message</td>
<td>%4 node process %5 exited after %1 seconds. Minimum required uptime for %5 process is %2 seconds. Delaying process restart for %3 seconds.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Process %5 exited after running for %1 seconds. Such processes must run for at least %2 seconds before the Node Manager will automatically restart them after they terminate. The Node Manager will restart the process after delaying %3 seconds for other environmental changes to complete.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>102C10A</td>
<td>Message</td>
<td>%2 node restarting process %3 after having delayed restart for %1 seconds.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Node Manager is restarting process %3 after the requisite delay of %1 seconds.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>102C10B</td>
<td>Message</td>
<td>Terminating process %2.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The %1 Node Manager is terminating process %2.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>102C10C</td>
<td>Message</td>
<td>%1 node process %2 exited after having detected a software failure.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Process %2 exited (terminated itself) after it detected an internal software error.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>If the process continues to terminate itself, call the Support Center.</td>
</tr>
<tr>
<td>102C10D</td>
<td>Message</td>
<td>Process %2 on %1 has detected a failure. Node Manager is restarting the process.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified Process has detected a situation that requires it to request that the Node Manager restart it. This often indicates a problem external to the process itself (for example, some other process may have failed).</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Node Manager on the ICM node will restart the process. The node should be checked to assure it is online using rtttest. If the condition is common, the process logs must be examined for cause.</td>
</tr>
<tr>
<td>102C10E</td>
<td>Message</td>
<td>Process %2 on %1 went down for unknown reason. Exit code %3. It will be automatically restarted.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified Process exited (terminated) with the indicated exit code. This termination is unexpected and the process died for an unknown reason. It will be automatically restarted.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>102C10F</td>
<td>Message</td>
<td>Process %4 on %3 is down after running for %1 seconds. It will restart after delaying %2 seconds for related operations to complete.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Determine if process has returned to service or has stayed offline. If process is offline or bouncing determine the cause from logs.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>102C110</td>
<td>Message</td>
<td>%1 node process %2 successfully reinitialized after restart.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Process %2 was successfully restarted.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>102C111</td>
<td>Message</td>
<td>%1 node process %2 successfully started.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Process %2 was successfully started.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>102C112</td>
<td>Message</td>
<td>%1 node process %2 exited cleanly and requested that it be restarted by the Node Manager.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Process %2 terminated itself successfully and has requested that the Node Manager restart it.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>102C113</td>
<td>Message</td>
<td>%1 node process %2 exited from Control-C or window close.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Process %2 exited as a result of a CTRL-C request or a request to close the process's active window.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>102C114</td>
<td>Message</td>
<td>%1 node process %2 exited and requested that the Node Manager reboot the system.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Process %2 terminated itself successfully but, due to other conditions, has requested that the Node Manager reboot the machine.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>102D101</td>
<td>Message</td>
<td>%3 Node Manager exited after having been up for %1 seconds. Scheduling system reboot in %2 seconds.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Node Manager has itself exited after having run for %1 seconds. The machine will be rebooted after waiting %2 seconds.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>102D102</td>
<td>Message</td>
<td>%2 Node Manager exited after having been up for %1 seconds. Auto-reboot is disabled. Will attempt service restart.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Node Manager has itself exited after having run for %1 seconds. The machine cannot be rebooted since auto-reboot is disabled. The Node Manager will attempt to restart the service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>102D103</td>
<td>Message</td>
<td>%3 Node Manager requested reboot after having been up for %1 seconds. Scheduling system reboot in %2 seconds.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Node Manager has requested the machine be rebooted after having run for %1 seconds. The machine will be rebooted after waiting %2 seconds.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>102D104</td>
<td>Message</td>
<td>%2 Node Manager requested reboot after having been up for %1 seconds. Auto-reboot is disabled. Will attempt service restart.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Node Manager has requested the machine be rebooted after having run for %1 seconds. The machine cannot be rebooted since auto-reboot is disabled. The Node Manager Manager will attempt to restart the service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
</tbody>
</table>
### Message Delivery Events

**Table 73:**

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>102D105</td>
<td>Message</td>
<td>%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.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A Critical Process has requested a reboot after the service has been up for %1 seconds. The machine cannot be rebooted since Auto-reboot on Process Request is disabled. The Node Manager Manager will attempt to restart the service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>102D106</td>
<td>Message</td>
<td>%3 A Critical Process has requested a reboot after having been up for %1 seconds. Scheduling system reboot in %2 seconds.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A Critical Process has requested the machine be rebooted after having run for %1 seconds. The machine will be rebooted after waiting %2 seconds.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1040010</td>
<td>Message</td>
<td>Synchronizer timed out trying to establish connection to peer.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Verify reliable network connectivity on the private network. Call the Cisco Systems, Inc. Customer Support Center in the event of a software failure on the duplexed partner.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1040022</td>
<td>Message</td>
<td>Connectivity with duplexed partner has been lost due to a failure of the private network, or duplexed partner is out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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.</td>
</tr>
<tr>
<td>1040023</td>
<td>Message</td>
<td>Communication with peer Synchronizer established.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The MDS message synchronizer has established communication with its duplexed partner.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>104802A</td>
<td>Message</td>
<td>MDS Time Delivery Queue size is increasing, current size is %1, but will continue to send messages.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>MDS Time Delivery Queue size is increasing over time.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Ensure that the ICM/IPCC configuration (#agents, # skills/agent, #PGs) is within the supported limit.</td>
</tr>
<tr>
<td>10F8004</td>
<td>Message</td>
<td>Device %1 path changing to idle state.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>10F8005</td>
<td>Message</td>
<td>Device %1 path changing to active state.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The indicated device is using this side of the Central Controller for its active communication path.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>10F8007</td>
<td>Message</td>
<td>Device %1 path realignment failed.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The indicated device failed to realign its message stream to this side of the Central Controller.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>10F8008</td>
<td>Message</td>
<td>Device %1 disconnected.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The indicated device has been disconnected from this side of the Central Controller. This may be caused by a network problem or device failure.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Remedy network problems, if any. Call the Cisco Systems, Inc. Customer Support Center in the event of a software failure on the device.</td>
</tr>
<tr>
<td>10F800E</td>
<td>Message</td>
<td>Device %1 path reset.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The communication path between this side of the Central Controller and the indicated device has been reset to an initial state.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>10F800F</td>
<td>Message</td>
<td>Device %1 initializing message stream.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The indicated device is initializing its message stream with this side of the Central Controller.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>10F801D</td>
<td>Message</td>
<td>The Network communications between ICM Router and Peripheral Gateway or NIC %2 has been down for %1 minutes.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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.</td>
</tr>
<tr>
<td>12A0001</td>
<td>Message</td>
<td>Message Delivery Service (MDS) feed from the Router to the Logger has failed.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Message Delivery Service (MDS) feed from the Router to the Logger has failed. Indicates MDS event feed connection from ICM Router to CSFS process on the Logger has failed.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>12A0002</td>
<td>Message</td>
<td>MDS In Service</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Indicates MDS event feed connection from ICM Router to CSFS process has connected.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>If not planned startup of system, determine if event is due to process, network, or system failure.</td>
</tr>
<tr>
<td>12A4001</td>
<td>Message</td>
<td>SDDSN Registration has been completed with system: %1, process: %2, using unique ID: %3. The registered system can now send diagnostic data to the TAC via the SDDSN server.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A system (%1), via process (%2), connected to the SDDSN server has successfully registered as a valid endpoint using the unique ID (%3). The system can now start sending diagnostic event data to the central TAC using the SDDSN server.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12A4002</td>
<td>Message</td>
<td>SDDSN Unregistration was never received from system: %1, process: %2, using unique ID: %3. The registered system abruptly disconnected from the SDDSN server.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A system (%1), via process (%2), connected to the SDDSN server has failed to unregistered as a valid endpoint using the unique ID (%3). This indicates that the system abruptly disconnected from the SDDSN server.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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(%1). 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(%1) and the primary SDDSN server. Other scenarios include a simplex SDDSN server failure / lost TCP/IP connection or the system(%1) that was communicating with the SDDSN server has somehow failed.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12A4003</td>
<td>Message</td>
<td>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 to the TAC via the SDDSN server.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A system (%1), via process (%2), connected to the SDDSN server has successfully unregistered as a valid endpoint using the unique ID (%3). This indicates that the system gracefully disconnected from the SDDSN server.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12A400A</td>
<td>Message</td>
<td>The SDDSN server is missing, or has outdated, resource files and cannot decipher messages for product %1, (%3). Message ID = %2</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 support 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.).</td>
</tr>
<tr>
<td>12A4010</td>
<td>Message</td>
<td>The client system: %3, attempted to send an incompatible version %1 SDDSN event. The current version supported is %2.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>An event has been received by a client system using an incompatible version of the SDDSN protocol.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>The client system need 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.</td>
</tr>
</tbody>
</table>
## Router Events

Table 74:

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>105007D</td>
<td>Message</td>
<td>Peripheral %2 (ID %1) is on-line.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified peripheral is on-line to the ICM. Call and agent state information is being received by the Router for this site.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>105007E</td>
<td>Message</td>
<td>ACD/IVR %2 (ID %1) is off-line and not visible to the Peripheral Gateway. Routing to this site is impacted.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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.</td>
</tr>
<tr>
<td>10500D0</td>
<td>Message</td>
<td>Physical controller %2 (ID %1) is on-line.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Router is reporting that physical controller %2 is on-line.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>10500D1</td>
<td>Message</td>
<td>Peripheral Gateway %2 (ID %1) is not connected to the Central Controller or is out of service. Routing to this site is impacted.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Communication (network) between the Central Controller (Router) and the PG should be checked using 'ping' and 'tracert'. Must have visible high priority connection from PG to Router. CCAG process on Router and PGAG process on PG should be checked. PG may have been taken out of service for maintenance.</td>
</tr>
<tr>
<td>10500D2</td>
<td>Message</td>
<td>PG has reported that peripheral %2 (ID %1) is operational.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>PG has reported that peripheral %2 (ID %1) is operational.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>10500D3</td>
<td>Message</td>
<td>PG has reported that peripheral %2 (ID %1) is not operational.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check that the peripheral is not off-line and that the connection from the peripheral to the PG is intact.</td>
</tr>
<tr>
<td>10500F6</td>
<td>Message</td>
<td>ScriptTable %2 (ID %1) is available only on side A.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>ScriptTable %2 is only available on the side A Router. If the side A Router goes down, no DB Lookup requests can be processed as side B cannot access the ScriptTable.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Configure a ScriptTable on side B that is identical to that on side A.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>10500F7</td>
<td>Message</td>
<td>ScriptTable %2 (ID %1) is available only on side B.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>ScriptTable %2 is only available on the side B Router. If the side B Router goes down, no DB Lookup requests can be processed as side A cannot access the ScriptTable.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Configure a ScriptTable on side B that is identical to that on side A.</td>
</tr>
<tr>
<td>10500F8</td>
<td>Message</td>
<td>ScriptTable %2 (ID %1) is not available on either side.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>No DB Lookup requests can be processed as ScriptTable %2 is unavailable on either side of the central controller.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Configure a ScriptTable on either side A or side B, preferably both.</td>
</tr>
<tr>
<td>10500F9</td>
<td>Message</td>
<td>ScriptTable %2 (ID %1) is available on both sides A and B.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>ScriptTable %2 is configured on both sides of the central controller.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>10500FF</td>
<td>Message</td>
<td>Side %1 %2 process is OK.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Router is reporting that side %1 process %2 is OK.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1050100</td>
<td>Message</td>
<td>Process %2 at the Central Site side %1 is down.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>10501F1</td>
<td>Message</td>
<td>ICM Node %2 (ID %1) is on-line.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified node is on-line to the ICM.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>10501F2</td>
<td>Message</td>
<td>ICM Node %2 (ID %1) is off-line.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified node is not visible to the ICM. Distribution of real time data may be impacted.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>10501F6</td>
<td>Message</td>
<td>The router's state size of %1 mb is now below the alarm limit of %2 mb.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The router's state size of %1 mb is now below the alarm limit of %2 mb.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>10501F7</td>
<td>Message</td>
<td>The router's state size of %1 mb has grown beyond the alarm limit of %2 mb.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>The alarm limit can be raised with the 'rtsetting' tool.</td>
</tr>
<tr>
<td>10501F8</td>
<td>Message</td>
<td>ICM Node %2 (ID %1) on system %3 is on-line.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified node is on-line to the ICM.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>10501F9</td>
<td>Message</td>
<td>ICM Node %2 (ID %1) on system %3 is off-line.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified node is not visible to the ICM. Distribution of real time data may be impacted. It is normal for this condition to 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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check the communication paths that connect the router and the node.</td>
</tr>
<tr>
<td>10501FD</td>
<td>Message</td>
<td>The router has completed loading the initial configuration from the logger.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified node is on-line to the ICM.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>10501FE</td>
<td>Message</td>
<td>The router has not loaded a configuration from the logger.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>This condition indicates that the router has not yet completed the initialization step of loading a configuration from the logger. It is normal for this condition to exist briefly while the system is loading. If it does not clear, it may indicate a problem with the logger machine or the communications paths that connect the router and logger.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check the communication paths that connect the router and the node.</td>
</tr>
<tr>
<td>105023C</td>
<td>Message</td>
<td>The router has detected that it is no longer synchronized with its partner.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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.</td>
</tr>
<tr>
<td>105029D</td>
<td>Message</td>
<td>Total number of Agent Skillgroup pair count %1 is exceeding the defined system default limit %2.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Total number of Agent Skillgroup pair count exceeds the defined system default limit.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Logout agents or remove skill group associated to the agent such that the agent skillgroup pair count does not exceed the defined system default limit.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>12B0013</td>
<td>Message</td>
<td>Application Gateway has failed. Application Gateway ID = %1</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>First determine why the application gateway process cannot connect to the host. Either the host process is not running or the communication link between the two machines is not working. Once this problem is fixed, use Application Gateway list tool in the Configuration Manager to take the application gateway process Out Of Service and then bring it back in service.</td>
</tr>
<tr>
<td>12B001F</td>
<td>Message</td>
<td>Application Gateway has connected with the host. Application Gateway ID = %1</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The application gateway is now connected to the host process.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12B0020</td>
<td>Message</td>
<td>Application Gateway is not connected to the host. Application Gateway ID = %1. Routing may be impacted.</td>
</tr>
</tbody>
</table>
## Logger Events

**Table 75:**

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>118C002</td>
<td>Message</td>
<td>%1%% of the available free space is used in %2 database.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>%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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Change the purge interval to save data for a shorter period of time. If this is not practical, add more disk to the system and add disk devices to the database by using SQL Server Management Studio.</td>
</tr>
<tr>
<td>118C00C</td>
<td>Message</td>
<td>%1%% of the available log space is used in %2 database.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>%1%% of the available log space is used in %2 database.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>118C00F</td>
<td>Message</td>
<td>Begin Automatic Purge: %1%% of the available data space is used in %2 database.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>118C010</td>
<td>Message</td>
<td>Automatic Purge Complete: %1%% of the available data space is used in the %2 database.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>118C015</td>
<td>Message</td>
<td>Connected To Client system %1 on port %2.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Logger successfully connected to a client system.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>118C017</td>
<td>Message</td>
<td>Logger or HDS connection to client system %1 on port %2 either went out of service or has been broken.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Logger or HDS on the specified TCP/IP connection and port number either went out of service or communication has been broken.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 HDS may have been shut down or otherwise disabled.</td>
</tr>
<tr>
<td>118C033</td>
<td>Message</td>
<td>Cannot find Routing Client with NetworkRoutingClient %1 on Server %2 in Database %3, Unable to Replicate Data to Customer %4 on CICR Instance %5</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CICR Replication must find a Routing Client in the database with a matching NetworkRoutingClient. Otherwise it cannot translate the RoutingClientId Foreign Key in the Dialed Number or Label properly. CICR Replication is unable to complete the replication in this case.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>118C034</td>
<td>Message</td>
<td>Cannot find Customer %1 or Instance %2 on Server %3 in Database %4. Unable to Replicate to Customer %1 on CICR Instance %2</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CICR Replication must find a Customer and Instance in the database with matching names. Otherwise it cannot translate the CustomerDefinitionID Foreign Key in the Dialed Number or Label properly. CICR Replication is unable to complete the replication in this case.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>118C035</td>
<td>Message</td>
<td>Dialed Number or Label Exists with Duplicate Key on Server %1 in Database %2, Unable to Replicate to Customer %3 on CICR Instance %4</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>118C036</td>
<td>Message</td>
<td>Duplicate Key Exists for Dialed Number with EnterpriseName %1</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>118C037</td>
<td>Message</td>
<td>Duplicate Key Exists for Dialed Number with RoutingClientID %1 and DialedNumberString %2</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CICR Replication has found that a Dialed Number already exists with this RoutingClientID and DialedNumberString. Therefore it cannot insert the new Dialed Number. CICR Replication is unable to complete the replication in this case.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>118C038</td>
<td>Message</td>
<td>Duplicate Key Exists for Label with RoutingClientID %1 and LabelString %2.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CICR Replication has found that a Label already exists with this RoutingClientID and LabelString. Therefore it cannot insert the new Label. CICR Replication is unable to complete the replication in this case.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>118C039</td>
<td>Message</td>
<td>CICR Replication on Side%1 is now Active.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CICR Replication Process is Active.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>118C03A</td>
<td>Message</td>
<td>CICR Replication on Side%1 is now Inactive.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CICR Replication Process is Inactive.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>118C03D</td>
<td>Message</td>
<td>INVALID Hostname is configured for %1 customer. Use Config ICM tool to re-configure the hostname for %1 customer.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Invalid hostname has been configured for the customer.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Use the Config[ICR-]ICR_NODE to change the hostname or system name and re-start the CICR replication process.</td>
</tr>
<tr>
<td>118C03E</td>
<td>Message</td>
<td>CICR Replication FAILED to Update CICR instance %1 due to CommitUpdateCCTransaction failure. Unable to Replicate to Customer %1. Check and correct the errors.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CICR Replication FAILED to update the configuration change due to the error caused by the CommitUpdateCCTransaction failure.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>118C040</td>
<td>Message</td>
<td>Found %1 records with DateTime greater than current Central Controller Time %2 in %3 table. Check and correct the errors.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Found historical records with DateTime greater than current Central Controller Time. Delete the records which have date time greater than the current central controller time.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>118C048</td>
<td>Message</td>
<td>NICR Replication on Side%1 is now Inactive.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NICR Replication Process is Inactive.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>
Peripheral Gateway (PG) Events

Table 76:

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>118C049</td>
<td>Message</td>
<td>NICR Replication on Side%1 is now Active.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NICR Replication Process is Active.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>118C051</td>
<td>Message</td>
<td>INVALID Hostname (%1) is configured for primary distributor for %2 customer. Use Config ICM tool to re-configure the primary distributor for %2 customer.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Use the ConfigICR-/ICR_NODE to change the hostname or system name and re-start the CICR replication process. Alternatively, check name resolution for the specified hostname.</td>
</tr>
</tbody>
</table>

Peripheral Gateway (PG) Events

Table 76:

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>108C020</td>
<td>Message</td>
<td>The Enterprise CTI Server associated with this Peripheral Gateway is on-line on %1.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>108C021</td>
<td>Message</td>
<td>The Enterprise CTI server associated with this Peripheral Gateway is down.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Look at the CTI server events and logs.</td>
</tr>
<tr>
<td>12E8006</td>
<td>Message</td>
<td>CONNECTION MONITOR SERVICE: Enterprise CTI session established by Client %1 (%2) at %3.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>An Enterprise CTI session has been opened by ClientID %1 (Signature %2) from IP address %3.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12E8007</td>
<td>Message</td>
<td>CONNECTION MONITOR SERVICE: Enterprise CTI session closed by Client %1 (%2) at %3.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Enterprise CTI session with ClientID %1 (Signature %2) at IP address %3 has been closed by the client.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>This indicates that an Enterprise CTI Client application that is normally always connected to the Enterprise CTI Server has closed its connection. The CTI Client application software may need to be checked for proper operation.</td>
</tr>
<tr>
<td>12E8008</td>
<td>Message</td>
<td>CONNECTION MONITOR SERVICE: Enterprise CTI session terminated with Client %1 (%2) at %3.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Enterprise CTI session with ClientID %1 (Signature %2) at IP address %3 has been terminated by the Enterprise CTI Server.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>This indicates that an Enterprise CTI Client application that is normally 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.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>12E800C</td>
<td>Message</td>
<td>Client:%1 Object:%2 Normal Event Report: %3</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Enterprise CTI client %1 application software has reported the following normal event for object %2: %3.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12E800D</td>
<td>Message</td>
<td>Client:%1 Object:%2 Warning Event Report: %3</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Enterprise CTI client %1 application software has reported the following warning for object %2: %3.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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.</td>
</tr>
<tr>
<td>12E800E</td>
<td>Message</td>
<td>Client:%1 Object:%2 Error Event Report: %3</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Enterprise CTI client %1 application software has reported the following error for object %2: %3.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>This indicates that the CTI Client application software has detected an error condition and may need to be checked for proper operation.</td>
</tr>
<tr>
<td>12E800F</td>
<td>Message</td>
<td>A Version 13 or prior CTI ClientID %1 (%2) at %3 connected with Agent multi line ENABLED.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check with the vendor of the software and see if they have ensured compatibility.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>12E8010</td>
<td>Message</td>
<td>A Version 13 or prior CTI ClientID %1 (%2) at %3 disconnected with Agent multi line ENABLED.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check with the vendor of the software and see if they have ensured compatibility.</td>
</tr>
<tr>
<td>13E0002</td>
<td>Message</td>
<td>Message Integration Service (MIS) was unable to connect to %1%2 on %3 TCP/IP Port %4.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Message Integration Service was unable to connect to the indicated component and address.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Confirm Component is available, Configuration of IP address(es) and Port(s) are correct, and Network connectivity would allow for connection</td>
</tr>
<tr>
<td>13E0003</td>
<td>Message</td>
<td>Connection to %1%2 on Address[%3:%4] Succeeded.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Message Integration Service was able to connect to the indicated component and address.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>13E0004</td>
<td>Message</td>
<td>Message Integration Service (MIS) was unable to open a session to %1%2.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Message Integration Service was unable to open a session to the indicated component</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>13E0005</td>
<td>Message</td>
<td>Session to %1%2 Opened.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Message Integration Service was able to open a session to the indicated component and address.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>13E0006</td>
<td>Message</td>
<td>TrunkGroup:%1 Trunk:%2 Received in Msg from Vru-%3 Not Configured</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A message pertaining to the indicated trunk group and trunk has not been configured with MIS</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Configure Extension, Trunk Group, and Trunk in MIS</td>
</tr>
<tr>
<td>13E0007</td>
<td>Message</td>
<td>Call Tracking Error: %1</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A call within MIS could not be tracked successfully.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Determine where tracking problem occurred and correct (For MIS problem could be MIS, VRU, or PG)</td>
</tr>
<tr>
<td>1540002</td>
<td>Message</td>
<td>An error occurred on the TCP/IP connection between the ACMI ACD Server(CTI) and the ACMI peripheral gateway. ACMI peripheral gateway is offline.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>An error occurred on the connection between the ACMI ACD Server(CTI) and the ACMI peripheral gateway. ACMI peripheral gateway is offline.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>If ACMI peripheral gateway does not re-attach contact the Support Center.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1540003</td>
<td>Message</td>
<td>Peripheral status was DOWN, going NORMAL. ACMI peripheral gateway is online.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Peripheral status was DOWN, going NORMAL. ACMI peripheral gateway is online.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1540007</td>
<td>Message</td>
<td>The route register on the DN %1 is Operational.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The DN is Operational.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1540008</td>
<td>Message</td>
<td>The route register failed for DN %1.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Permit Application Routing box on the child system is not checked for DN.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check Permit Application Routing box.</td>
</tr>
<tr>
<td>1540009</td>
<td>Message</td>
<td>The route register failed for DN %1.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Add the DN on Child System and Ensure that Permit application routing is enabled.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>154000A</td>
<td>Message</td>
<td>The route register failed for DN %1.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Add the DN on Child System and Ensure that Permit application routing is enabled.</td>
</tr>
<tr>
<td>154000B</td>
<td>Message</td>
<td>The route register failed for DN %1.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>You have specified an incorrect Server Peripheral ID in the PG Setup of the Gateway PG.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Correct the Server Peripheral ID in the PG Setup of the Gateway PG and Cycle the PG.</td>
</tr>
<tr>
<td>154000C</td>
<td>Message</td>
<td>The route register failed for DN %1.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Another Gateway PG has requested control of this DN - Likely incorrect Server hostname configured.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Correct the Server host name in the PG Setup of the Gateway PG and Cycle the PG.</td>
</tr>
<tr>
<td>154000D</td>
<td>Message</td>
<td>The peripheral id %1 given is not valid.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>You have specified an incorrect Server Peripheral ID in the PG Setup of the Gateway PG.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Correct the Server Peripheral ID in the PG Setup of the Gateway PG and Cycle the PG.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>154000E</td>
<td>Message</td>
<td>Central Controller Connection on Child Down - ACMI peripheral gateway status DOWN.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Central Controller Connection on Child Down - ACMI peripheral gateway status DOWN.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1560004</td>
<td>Message</td>
<td>CTI OS Server version %2 is online. Connected to CTI Server at %3. CTI Server protocol is %1.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Message indicating the version of CTI OS Server as well as the protocol version CTI OS Server uses to connect to CTI Server.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1560005</td>
<td>Message</td>
<td>CTI OS Server version %2 cycled because the connection to CTI Server at %3 closed. CTI Server protocol is %1.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 Cisco customer support.</td>
</tr>
<tr>
<td>1560006</td>
<td>Message</td>
<td>CTI OS Server version %2 cycled because the connection to CTI Server at %3 failed. CTI Server protocol is %1.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 with the SRND to make sure it is within tolerance.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1560007</td>
<td>Message</td>
<td>CTI OS Server has %1 messages in Queue.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CTI OS Server incoming message is now below 10000 messages.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1560008</td>
<td>Message</td>
<td>CTI OS Server has %1 messages in Queue.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CTI OS Server incoming message queue exceeded 10000 messages. This might result in unwanted behavior.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 with the SRND to make sure it is within tolerance.</td>
</tr>
<tr>
<td>1560009</td>
<td>Message</td>
<td>CTI OS Server has generated an exception in %2 processing a %3.\nDetails:\n%4: %1\n%5</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CTI OS Server generated an exception while processing a request or an event specified in this method.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 Cisco customer support.</td>
</tr>
<tr>
<td>156000A</td>
<td>Message</td>
<td>CTI OS Server has generated an exception in %2 processing %3.\nDetails:\n%4: %1\n%5</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CTI OS Server generated an exception while processing the request or event specified in this method.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 Cisco customer support.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>156000B</td>
<td>Message</td>
<td>CTI OS Server's total amount of agent mode connections is %1. This is within CTI OS Server's limit of %2.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CTI OS Server is currently running with an acceptable number of agents connected to it.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required</td>
</tr>
<tr>
<td>156000C</td>
<td>Message</td>
<td>CTI OS Server's total amount of agent mode connections is %1. This exceeds CTI OS Server's limit of %2.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CTI OS Server is currently running with an excessive number of agents connected to it.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Ensure that the number of agents 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 half the number of agents that can connect to CTI OS Server.</td>
</tr>
<tr>
<td>156000D</td>
<td>Message</td>
<td>CTI OS Server's total amount of monitor mode connections is %1. This is within CTI OS Server's limit of %2.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CTI OS Server is currently running with an acceptable number of monitor-mode applications connected to it.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>156000E</td>
<td>Message</td>
<td>CTI OS Server's total amount of monitor mode connections is %1. This exceeds CTI OS Server's limit of %2.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CTI OS Server is currently running with an excessive number of monitor-mode applications connected to it.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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.</td>
</tr>
<tr>
<td>156000F</td>
<td>Message</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CTI OS Server has re-enabled monitor mode functionality.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1560010</td>
<td>Message</td>
<td>CTI OS Server's monitor mode functionality has been disabled after %1 failed attempts to access monitor mode functionality.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 [ip_address] 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).</td>
</tr>
</tbody>
</table>

<p>| 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. |</p>
<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1560012</td>
<td>Message</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 Cisco customer support.</td>
</tr>
<tr>
<td>1560013</td>
<td>Message</td>
<td>CTI OS Server is Within limit for %1%2. %3</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CTI OS Server is Within the operational limit for this configuration/action.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1560014</td>
<td>Message</td>
<td>CTI OS Server limit for %1%2 has been violated. %3</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CTI OS Server operational limit has been violated</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>This event occurs when a CTI OS Server operational limit has been violated for either a configuration or action. This violation may adversely effect CTI OS performance. Please check the published operational limits for this release of CTI OS Server.</td>
</tr>
</tbody>
</table>
## Administrator Workstation Events

**Table 77:**

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>106003A</td>
<td>Message</td>
<td>World Wide Web Publishing Service may be down. ICM cannot communicate with web server.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>World Wide Web Publishing Service may be down. ICM cannot communicate with web server.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Start World Wide Web Publishing Service if it is not running. Otherwise, look for messages in the IIS error log.</td>
</tr>
<tr>
<td>106003B</td>
<td>Message</td>
<td>World Wide Web Publishing Service is up.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>World Wide Web Publishing Service is up.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

## Outbound Option Events

**Table 78:**

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1438000</td>
<td>Message</td>
<td>Blended Agent Campaign Manager on [%1] is down.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Blended Agent 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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Make sure the Campaign Manager process is enabled in the registry. Also, check that the Blended Agent database server is running. The Blended Agent private database should have been created with the ICMDBA tool.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1438001</td>
<td>Message</td>
<td>Blended Agent Campaign Manager on [%1] is up.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Blended Agent Campaign Manager is ready to distribute customer records and configuration data.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1438002</td>
<td>Message</td>
<td>Failed to execute import into table [%1] due to a change in the tables' schema.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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.</td>
</tr>
<tr>
<td>1438003</td>
<td>Message</td>
<td>Import failed due to an invalid table [%1] definition.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Could not create the specified table due to invalid import schema definition.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check that all table columns for the failed import are correct. Making a character column too long could cause this failure.</td>
</tr>
<tr>
<td>1438004</td>
<td>Message</td>
<td>Failed to import data into table [%1].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>This error could occur if the import file did not match the table definition.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check that the import table definition matches the import file.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1438005</td>
<td>Message</td>
<td>Failed to build dialing list from table [%1].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A Dialing list could not be populated from the specified table.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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.</td>
</tr>
<tr>
<td>1438006</td>
<td>Message</td>
<td>Could not open [%1] database.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Blended Agent private database has not been initialized or SQL Server is not running.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Make sure SQL Server is running. Check the ODBC configuration settings for the Blended Agent private database. Was the ICMDBA tool run to create the Blended Agent private database?</td>
</tr>
<tr>
<td>1438007</td>
<td>Message</td>
<td>An import was started but it's configuration was deleted while it was running.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>An import started running but part of it's configuration was deleted before it was able to do anything.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Reschedule the import.</td>
</tr>
<tr>
<td>1438008</td>
<td>Message</td>
<td>Blended Agent CTI Server connection on computer [%1] is down.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Blended Agent CTI Server connection has been terminated.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Make sure CTI Server is active. Also make sure the PIM has connectivity to the switch.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1438009</td>
<td>Message</td>
<td>Blended Agent CTI Server connection on computer [%1] is active.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Blended Agent CTI Server connection is active.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1438010</td>
<td>Message</td>
<td>Dialer telephony port [%1] is not functioning correctly.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 cards ID is assigned by a hardware switch on the top of the card. Ports are numbered consecutively across all ports.</td>
</tr>
<tr>
<td>1438011</td>
<td>Message</td>
<td>Blended Agent telephony port [%1] has recovered.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A previously malfunctioning telephony port has received a message from the telephony driver indicating the port is back in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1438012</td>
<td>Message</td>
<td>BAImport is down on the computer [%1].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>BAImport is not running on the specified computer.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please check that the Import process has not been shutdown. Check that the BA Private database has been created. Also, check that SQL Server is running.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1438013</td>
<td>Message</td>
<td>BAImport is up on the computer [%1].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>BAImport is running on the specified computer.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1438014</td>
<td>Message</td>
<td>Dialer is down on the computer [%1].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Dialer is down on the specified computer.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please check that the Dialogic drivers are configured and running. Also verify that the Dialer has been started by Node Manager.</td>
</tr>
<tr>
<td>1438015</td>
<td>Message</td>
<td>Dialer is up on the computer [%1].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Dialer is up on the specified computer.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1438018</td>
<td>Message</td>
<td>Failed to rename or delete the import file for Import Rule Id: %1. 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.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Failed to rename or delete the import file for Import Rule Id: [id; filename]. 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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1438019</td>
<td>Message</td>
<td>Campaign [%1] trying to [%2] and database timed out.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Campaign [campaign name] tried to run a query [query name] and database timed out.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1438020</td>
<td>Message</td>
<td>Database is running out of space.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Database is running out of space.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please create some space in the database.</td>
</tr>
<tr>
<td>1438021</td>
<td>Message</td>
<td>The Agent SkillGroup [%1] recieved is not the configured SkillGroup [%2] for the Campaign [%3].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Agent Skill group recievied is not configured for this Campaign.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Make Sure the Skill Group configured in the script is the same as the Skill Group configured in the Campaign.</td>
</tr>
<tr>
<td>1438022</td>
<td>Message</td>
<td>Timeout happening for the call on Port [%1]. Time to get the MR response : [%2 seconds].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Timeout happening for the call on Port.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Timeout happening for a call on Port. Check the Registry Key TimeToWaitForMRIResponse.</td>
</tr>
<tr>
<td>1438023</td>
<td>Message</td>
<td>Media Routing PIM Disconnected with the Dialer [%1].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Media Routing PIM Disconnected with the Dialer.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check whether the MR PIM is active or not.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1438024</td>
<td>Message</td>
<td>MR PIM connected to Dialer [%1].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>MR PIM connected to Dialer [dialer name].</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1438025</td>
<td>Message</td>
<td>Import ID [%1] has more than 10000 Errors.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Import Process has more than 10000 Errors.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Restart the Import Process.</td>
</tr>
<tr>
<td>1438026</td>
<td>Message</td>
<td>Dialer [%1] with incorrect protocol version trying to connect.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Dialer with incorrect protocol version trying to connect.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please check the Dialer version.</td>
</tr>
<tr>
<td>1438027</td>
<td>Message</td>
<td>Campaign [%1] DNC list to be imported has exceeded the total number of DNC Records allowed. Please check the CampaignManager log files for more details.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The DNC List to be imported has exceeded the number of DNC Records set by ConfigLimit</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please check the DNC record limit set by the ConfigLimit tool.</td>
</tr>
<tr>
<td>1438028</td>
<td>Message</td>
<td>For %1 process System Out Of Memory.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Memory Overflow. Not able to instantiate or assign enough memory.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>This is a memory outage, and the configuration of the system may not be sufficient.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1438029</td>
<td>Message</td>
<td>Dialer: Unknown Port Owner [%1]</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Dialer: Unknown Port Owner.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please check the Administrator scripts.</td>
</tr>
<tr>
<td>1438030</td>
<td>Message</td>
<td>Cannot find key [%1] in the Registry.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Cannot find key in the Registry.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please ensure that the installation process went smooth.</td>
</tr>
<tr>
<td>1438031</td>
<td>Message</td>
<td>Unable to open Registry key: [%1]</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Unable to open Registry key.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please ensure that the installation process went smooth.</td>
</tr>
<tr>
<td>1438032</td>
<td>Message</td>
<td>Campaign Manager could not connect to the BA private Database.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Campaign Manager could not connect to the BA private Database.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Make sure the SQL Server is running and the Blended Agent private database is initialized.</td>
</tr>
<tr>
<td>1438033</td>
<td>Message</td>
<td>Dialer attempted to connect to incorrect Campaign Manager version [%1], required version [%2]</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Dialer attempted to connect to incorrect Campaign Manager version.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please ensure that the CampaignManager is compatible with the Dialer Version.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1438034</td>
<td>Message</td>
<td>Your configured dialer type [%1] doesn't match this dialer type [%2]</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Your configured dialer type doesn't match this dialer type.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please check the dialer type configured. IP or SIP.</td>
</tr>
<tr>
<td>1438035</td>
<td>Message</td>
<td>Dialer has too many ports configured [%1], maximum allowed [%2]</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Dialer has too many ports configured.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please decrease the number of Ports configured.</td>
</tr>
<tr>
<td>1438036</td>
<td>Message</td>
<td>Campaign Manager: Unable to convert System Time to FileTime</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Campaign Manager: Unable to convert System Time to FileTime</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1438037</td>
<td>Message</td>
<td>Blended Agent connection to SIP Server [%1] on computer [%2] is down, heart beat failure detected</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Blended Agent SIP Server heart beat failure, the connection is down.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please make sure SIP Server is alive and reachable from Blended Agent SIP dialer.</td>
</tr>
<tr>
<td>1438038</td>
<td>Message</td>
<td>Blended Agent connection to SIP Server [%1] on computer [%2] is up, heart beat ack. detected</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Blended Agent SIP Server heart beat ack. received, the connection is up</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1438039</td>
<td>Message</td>
<td>Current private database version is [%1]. Required version is [%2].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Blended Agent private database version is not correct. It needs to be upgraded using EDMT.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please upgrade private database to the correct version using EDMT for this release.</td>
</tr>
<tr>
<td>1438040</td>
<td>Message</td>
<td>Missing\incorrect local Static Route File is detected on [%1] in the directory, ..\icm[%2]\Dialer].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Static route file, ..\Dialer\DNPHost, is missing or has no valid static route entry when configuring the SIP Dialer to connect to voice Gateway.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Re-run the Dialer setup to install smaple DNPHost file, and/or enter valid static route entry.</td>
</tr>
<tr>
<td>1438041</td>
<td>Message</td>
<td>CPA is disabled on voice gateway [%1], Number of calls without CPA: [%2].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CPA is disabled or not supported on voice gateway.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please enable CPA on voice gateway.</td>
</tr>
<tr>
<td>1438042</td>
<td>Message</td>
<td>Action Required : BA Db Space Availability Remaining is very less: [%1%%]</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>BA Database Space Utilization has reached the Threshold Limit.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please increase the DB space utilization or remove unnecessary records from the BA Database.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1438043</td>
<td>Message</td>
<td>[%1] has insufficient records [%2] in the last one minute on the dialer machine [%3]</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Campaign skill group has insufficient customer records.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please increase the 'records to cache' from the Campaign configuration.</td>
</tr>
<tr>
<td>1438044</td>
<td>Message</td>
<td>Voice Gateway has been overdialed in the last [%1] seconds. Resource Not Available Rate is %2%, Configured-Current Port Throttle: [%3].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The capacity of Voice Gateway or Carrier has been exceeded.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please check the capacity of Voice Gateway or Carrier, and adjust the value of 'Port Throttle' from the Dialer Configuration accordingly.</td>
</tr>
<tr>
<td>1438045</td>
<td>Message</td>
<td>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].</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Single-state Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>SIP Dialer decreases the port throttle since the capacity of Voice Gateway or Carrier is exceeded.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Please adjust the value of 'Port Throttle' from the Dialer configuration or check BOM to do proper sizing calculation for Outbound Dialer.</td>
</tr>
</tbody>
</table>
## ICM Network Interface Controller (NIC) Events

**Table 79:**

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>10D800A</td>
<td>Message</td>
<td>SS7 linkset %1 unavailable.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 linkset to the AT&amp;T network is now in a non-working state. This means that all links (normally one, but possibly more) between the NIC and a particular Signal Transfer Point (STP) in the AT&amp;T network are not operational. This is most likely due to a circuit problem in either the Local Exchange Carrier or in the AT&amp;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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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&amp;T Advanced Features Services Center (AFDSC) at 800-621-6901. Ask to speak to an ICP technician.</td>
</tr>
<tr>
<td>10D800B</td>
<td>Message</td>
<td>SS7 linkset %1 available.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 linkset to the AT&amp;T network is now in a working state.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>10D8010</td>
<td>Message</td>
<td>SS7 network accessible. DPC=%1</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The interface to the AT&amp;T network has returned to a working state. At least one link is now operational, although others may still be down.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>10D8011</td>
<td>Message</td>
<td>SS7 network inaccessible. DPC=%1</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>All links to the ATworT 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 ATotiT 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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 ATd aT Advanced Features Service Center (AFSC) at 800-621-6901. Ask to speak to an ICP technician. If you have provisioned alternate A-links, use your ATbleT network routing application, e.g. Routing Manager, to redirect traffic to the alternate CRP which uses the alternate links.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>10D8101</td>
<td>Message</td>
<td>ICP Gateway ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>10D8102</td>
<td>Message</td>
<td>NIC ICP Gateway has stopped operation due to the following \ error ( %1 ). Calls will be default routed.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>10D8106</td>
<td>Message</td>
<td>Routing Client %1 STOPPED. (%2)</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified Routing 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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 Customer Service Center.</td>
</tr>
<tr>
<td>10D8107</td>
<td>Message</td>
<td>Routing Client %1 ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified Routing Client is now fully operational and able to process calls for the associated subsystem/CRP-ID.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1168200</td>
<td>Message</td>
<td>SPRGATE ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>SPRCommStart() which begins execution of the Gateway has returned without error.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1168201</td>
<td>Message</td>
<td>SPRGATE OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>SPRGate is halting execution.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>116C100</td>
<td>Message</td>
<td>SPRCOMM Link %1 to SCP %2 OPEN.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Link State is changing from LINK_OPENING to LINK_OPEN.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>116C101</td>
<td>Message</td>
<td>The Sprint Service Control Point ( SCP ) %1 to ( %2 ) is either out of service or communications between ICM and the SCP has broken.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Sprint Service Control Point is either out of service or communications between ICM and the SCP has broken. All connections associated with this link are about to be closed.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>The connection between the Router and Sprint has failed. If all Service Control Points (SCPs) are disconnected from the Router then ICM is not routing calls. Sprint should be contacted for resolution.</td>
</tr>
<tr>
<td>1288002</td>
<td>Message</td>
<td>SS7 link %1 in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1288003</td>
<td>Message</td>
<td>SS7 link %1 out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>128800A</td>
<td>Message</td>
<td>SS7 linkset %1 unavailable.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>128800B</td>
<td>Message</td>
<td>SS7 linkset %1 available.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1288101</td>
<td>Message</td>
<td>BTNIC Gateway ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1288102</td>
<td>Message</td>
<td>BTNIC Gateway STOPPED. (%1)</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 Support Center should be alerted to investigate and correct the problem.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>12D800A</td>
<td>Message</td>
<td>Network ICM %1 is now accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The ICRP NIC has established its first communication session with the indicated Network ICM. This indicates that network connectivity exists to the indicated NICR.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12D800B</td>
<td>Message</td>
<td>Network ICM %1 is no longer accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The ICRP NIC no longer has any communication sessions established with the indicated Network ICM. This points to a problem with the indicated NICR, or a problem with network connectivity.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>ICRP Network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>12F8009</td>
<td>Message</td>
<td>SCP [%1:%2] is now accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NORTEL NIC has established a communication session with the indicated SCP. This indicates that network connectivity exists to the indicated SCP.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12F800A</td>
<td>Message</td>
<td>SCP [%1:%2] is no longer accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NORTEL NIC has disconnected the communication sessions established with the indicated SCP.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Nortel network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>12F800C</td>
<td>Message</td>
<td>SCP [%1:%2] Accessible But Session to Other Side SCP[%1:%3] is still Active.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Determine cause of Failover</td>
</tr>
<tr>
<td>12F8200</td>
<td>Message</td>
<td>NTGATE ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NORTEL NIC is online and is prepared to accept route requests from the Nortel network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12F8201</td>
<td>Message</td>
<td>NTGATE OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NORTEL NIC is offline and cannot accept route requests from the Nortel network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1340017</td>
<td>Message</td>
<td>Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>INAP NIC was unable to connect to the GATEWAY on the INAP network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity would allow for connection</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1348009</td>
<td>Message</td>
<td>GATEWAY [%1] is now accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The INAP NIC has established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>134800A</td>
<td>Message</td>
<td>GATEWAY [%1] is no longer accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The INAP NIC has disconnected the communication sessions established with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>INAP network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>134800C</td>
<td>Message</td>
<td>GATEWAY [%1] is not accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Although connected, the INAP NIC cannot establish a session with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>INAP network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>1348200</td>
<td>Message</td>
<td>INAPGATE ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The INAP NIC is online and is prepared to accept route requests from the INAP network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1348201</td>
<td>Message</td>
<td>INAPGATE OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The INAP NIC is offline and cannot accept route requests from the INAP network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1358004</td>
<td>Message</td>
<td>INRCEngine (DeviceID=%1) Initiating Admission Control.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Routing Client Engine is refusing new calls due to a larger than normal 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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 Support Center should be alerted to investigate and correct the problem.</td>
</tr>
<tr>
<td>1358005</td>
<td>Message</td>
<td>INRCEngine (DeviceID=%1) Terminating Admission Control.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The backlog of calls that caused Admission Control to be initiated has now been reduced to an acceptable level. Normal call routing has resumed.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>135800A</td>
<td>Message</td>
<td>INRCEngine (DeviceID=%1) Initiating Restriction Control for CalledParty '%2'.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Routing Client Engine is restricting the rate of new calls with the indicated called party number prefix due to a larger than normal backlog of calls.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>135800B</td>
<td>Message</td>
<td>INRCEngine (DeviceID=%1) Terminating Restriction Control on CalledParty '%2'.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Routing Client Engine is no longer restricting calls with the indicated called party number prefix.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1368002</td>
<td>Message</td>
<td>SS7 link %1 in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1368003</td>
<td>Message</td>
<td>SS7 link %1 out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now out of service. This is most likely due</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to a circuit problem between the INAP Gateway and the adjacent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>signaling point to which this link connects. Equipment problems are</td>
</tr>
<tr>
<td></td>
<td></td>
<td>also a possible cause. Because each link typically belongs to a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>linkset containing two or more links, connectivity between the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INAP Gateway and the adjacent signaling point is not lost unless all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>other links in the linkset have failed. If this occurs, a 'linkset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unavailable' alarm is generated.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>136800A</td>
<td>Message</td>
<td>SS7 linkset %1 unavailable.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 linkset is now unavailable. This means that no</td>
</tr>
<tr>
<td></td>
<td></td>
<td>links in that linkset are operational. Consequently, communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>has failed between the INAP Gateway and the adjacent signaling point</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to which the linkset connects.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>136800B</td>
<td>Message</td>
<td>SS7 linkset %1 available.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 linkset is now available. At least one link in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>linkset is operational, although others may still be down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communication between the INAP Gateway and the adjacent signaling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>point to which the linkset connects has been restored.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1368014</td>
<td>Message</td>
<td>SS7 link %1 of linkset %2 is in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1368015</td>
<td>Message</td>
<td>SS7 link %1 of linkset %2 is out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>1368101</td>
<td>Message</td>
<td>INAP Gateway ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The INAP Gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1368102</td>
<td>Message</td>
<td>INAP Gateway STOPPED. (%1)</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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. 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 Support Center should be alerted to investigate and correct the problem.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>138800A</td>
<td>Message</td>
<td>Network ICM %1 is now accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The INCRP NIC has established its first communication session with the indicated Network ICM. This indicates that network connectivity exists to the indicated NICR.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>138800B</td>
<td>Message</td>
<td>Network ICM %1 is no longer accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The INCRP NIC no longer has any communication sessions established with the indicated Network ICM. This points to a problem with the indicated NICR, or a problem with network connectivity.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>INCRP Network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>139800A</td>
<td>Message</td>
<td>Network ICM %1 is now accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NEC NIC has established its first communication session with the indicated SCP. This indicates that network connectivity exists to the indicated SCP.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>139800B</td>
<td>Message</td>
<td>Network ICM %1 is no longer accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NEC NIC no longer has any communication sessions established with the indicated SCP. This points to a problem with the indicated SCP, or a problem with network connectivity.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>NEC Network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>13A8202</td>
<td>Message</td>
<td>Dialogue on SVC %1 is now OPEN.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A dialogue with the SCP is now open and available to carry traffic.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>13A8203</td>
<td>Message</td>
<td>Dialogue on SVC %1 is now CLOSED.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NIC has an existing SVC open to the SCP and is waiting for a dialogue open message. The NIC has waited for a configured amount of time and has not received a dialogue open message.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Determine if the SCP application is running and sending open requests.</td>
</tr>
<tr>
<td>13A8206</td>
<td>Message</td>
<td>FTGATE ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The France Telecom NIC is online and is prepared to accept route requests from the network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>13A8207</td>
<td>Message</td>
<td>FTGATE OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The France Telecom NIC is offline and cannot accept route requests from the network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>13F8200</td>
<td>Message</td>
<td>Session with Client Id %1 SCP index %2 configuration valid.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>If a configuration error has occurred, it is cleared when the session is closed.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>13F8201</td>
<td>Message</td>
<td>Session with Client Id %1 SCP index %2 configuration invalid.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Determine if the SCP is on line and if the communications links are available.</td>
</tr>
<tr>
<td>13F8202</td>
<td>Message</td>
<td>Session with Client Id %1 SCP index %2 is now OPEN.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A session with the SCP is now open and available to carry traffic.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>13F8203</td>
<td>Message</td>
<td>Session with Client Id %1 SCP index %2 is now CLOSED.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>No session is currently opened with the SCP. The SCP index indicates the relative position of that SCP's configuration in the NT Registry.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Determine if the SCP is on line and if the communications links are available.</td>
</tr>
<tr>
<td>13F8206</td>
<td>Message</td>
<td>CRSP GATE ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CRSP NIC is online and is prepared to accept route requests from the network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>13F8207</td>
<td>Message</td>
<td>CRSP GATE OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CRSP NIC is offline and cannot accept route requests from the network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>1428203</td>
<td>Message</td>
<td>SS7 link %1 in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1428204</td>
<td>Message</td>
<td>SS7 link %1 out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>142820B</td>
<td>Message</td>
<td>SS7 linkset %1 unavailable.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>142820C</td>
<td>Message</td>
<td>SS7 linkset %1 available.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1428210</td>
<td>Message</td>
<td>INAP Gateway ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The INAP Gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1428211</td>
<td>Message</td>
<td>INAP Gateway STOPPED. (%1)</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 Support Center should be alerted to investigate and correct the problem.</td>
</tr>
<tr>
<td>1428310</td>
<td>Message</td>
<td>SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1428311</td>
<td>Message</td>
<td>SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1428312</td>
<td>Message</td>
<td>SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>1428313</td>
<td>Message</td>
<td>SS7 linkset available (Gateway PC=%1, Linkset RPC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1440017</td>
<td>Message</td>
<td>Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>ENERGIS NIC was unable to connect to the GATEWAY on the ENERGIS network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity would allow for connection</td>
</tr>
<tr>
<td>1448009</td>
<td>Message</td>
<td>GATEWAY [%1] is now accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The ENERGIS NIC has established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>144800A</td>
<td>Message</td>
<td>GATEWAY [%1] is no longer accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The ENERGIS NIC has disconnected the communication sessions established with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>ENERGIS network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>144800C</td>
<td>Message</td>
<td>GATEWAY [%1] is not accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Although connected, the ENERGIS NIC cannot establish a session with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>ENERGIS network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>1448012</td>
<td>Message</td>
<td>SS7 link %1 in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1448013</td>
<td>Message</td>
<td>SS7 link %1 out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>144801A</td>
<td>Message</td>
<td>SS7 linkset %1 unavailable.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>144801B</td>
<td>Message</td>
<td>SS7 linkset %1 available.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1448101</td>
<td>Message</td>
<td>INAP Gateway ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The INAP Gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1448102</td>
<td>Message</td>
<td>INAP Gateway STOPPED. (%1)</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 Support Center should be alerted to investigate and correct the problem.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1448200</td>
<td>Message</td>
<td>ENERGISGATE ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The ENERGIS NIC is online and is prepared to accept route requests from the ENERGIS network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1448201</td>
<td>Message</td>
<td>ENERGISGATE OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The ENERGIS NIC is offline and cannot accept route requests from the ENERGIS network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1450017</td>
<td>Message</td>
<td>Session for Gateway[%1] Connect FAILED to Gateway at Port %2 at Address %3.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CAIN NIC unable to connect to the Gateway on the CAIN network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Confirm Gateway is available, configuration of IP address and Port are correct, and network connectivity allows for connection.</td>
</tr>
<tr>
<td>1458009</td>
<td>Message</td>
<td>Gateway[%1] is now accessible (GSP open response accepted).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CAIN NIC has established a communication session with the indicated Gateway. This indicates that network connectivity exists to the indicated Gateway.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>145800A</td>
<td>Message</td>
<td>Gateway[%1] is no longer accessible (GSP session closed).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CAIN NIC has disconnected the communication sessions established with the indicated Gateway.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>CAIN network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>145800C</td>
<td>Message</td>
<td>Gateway[%1] not accessible (no GSP open response returned); retrying...</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Although connected, the CAIN NIC cannot establish a session with the indicated Gateway.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>CAIN network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>1458200</td>
<td>Message</td>
<td>CAINGATE is now ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CAIN NIC is online and is prepared to accept route requests from the CAIN network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1458201</td>
<td>Message</td>
<td>CAINGATE is now OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CAIN NIC is offline and cannot accept route requests from the CAIN network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1458301</td>
<td>Message</td>
<td>SS7 link %1 of linkset %2 is in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1458302</td>
<td>Message</td>
<td>SS7 link %1 of linkset %2 is out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now out of service. This is most likely due to a circuit problem between the AIN 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 AIN 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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>1458309</td>
<td>Message</td>
<td>SS7 linkset %1 unavailable.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication has failed between the AIN Gateway and the adjacent signaling point to which the linkset connects.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>145830A</td>
<td>Message</td>
<td>SS7 linkset %1 available.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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 AIN Gateway and the adjacent signaling point to which the linkset connects has been restored.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1458400</td>
<td>Message</td>
<td>AIN Gateway ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The AIN Gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1458401</td>
<td>Message</td>
<td>AIN Gateway STOPPED. (%1)</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The AIN Gateway has stopped operation due to the specified error code. The AIN subsystem is prohibited. The network should adjust by sending calls to the Router through an alternate path utilizing a different AIN Gateway. This can be caused by a communication problem between the AIN Gateway and the NIC, by a problem with the Router, or by an administrative AIN Gateway command.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>This event can be caused by a transient problem which may be automatically corrected as indicated by a 'AIN Gateway online' event. If the problem persists for more than three minutes, the Support Center should be alerted to investigate and correct the problem.</td>
</tr>
<tr>
<td>1460017</td>
<td>Message</td>
<td>Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Unisource NIC was unable to connect to the GATEWAY on the Unisource network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity would allow for connection</td>
</tr>
<tr>
<td>1468009</td>
<td>Message</td>
<td>GATEWAY [%1] is now accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Unisource NIC has established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>146800A</td>
<td>Message</td>
<td>GATEWAY [%1] is no longer accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Unisource NIC has disconnected the communication sessions established with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Unisource network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>146800B</td>
<td>Message</td>
<td>GATEWAY [%1] is not accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Although connected, the Unisource NIC cannot establish a session with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Unisource network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>146800D</td>
<td>Message</td>
<td>SS7 link %1 in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>146800E</td>
<td>Message</td>
<td>SS7 link %1 out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>1468015</td>
<td>Message</td>
<td>SS7 linkset %1 unavailable.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1468016</td>
<td>Message</td>
<td>SS7 linkset %1 available.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1468017</td>
<td>Message</td>
<td>SS7 Gateway ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The SS7 Gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1468018</td>
<td>Message</td>
<td>SS7 Gateway STOPPED. (%1)</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 Support Center should be alerted to investigate and correct the problem.</td>
</tr>
<tr>
<td>1468200</td>
<td>Message</td>
<td>UNISOURCE Routing Client is ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Unisource NIC is online and is prepared to accept route requests from the Unisource network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1468201</td>
<td>Message</td>
<td>UNISOURCE Routing Client is OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The Unisource NIC is offline and cannot accept route requests from the Unisource network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1468310</td>
<td>Message</td>
<td>SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1468311</td>
<td>Message</td>
<td>SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1468312</td>
<td>Message</td>
<td>SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1468313</td>
<td>Message</td>
<td>SS7 linkset available (Gateway PC=%1, Linkset RPC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1468314</td>
<td>Message</td>
<td>SCTP connection is down (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1468315</td>
<td>Message</td>
<td>ASP is Down (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1468316</td>
<td>Message</td>
<td>ASP is Inactive (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1468317</td>
<td>Message</td>
<td>ASP is Active (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The ASP is Active. Calls can be processed through this connection.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1490017</td>
<td>Message</td>
<td>Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>CONCERT NIC was unable to connect to the GATEWAY on the CONCERT network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity would allow for connection</td>
</tr>
<tr>
<td>1498009</td>
<td>Message</td>
<td>GATEWAY [%1] is now accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CONCERT NIC has established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>149800A</td>
<td>Message</td>
<td>GATEWAY [%1] is no longer accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CONCERT NIC has disconnected the communication sessions established with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>CONCERT network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>149800C</td>
<td>Message</td>
<td>GATEWAY [%1] is not accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Although connected, the CONCERT NIC cannot establish a session with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>CONCERT network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>1498200</td>
<td>Message</td>
<td>CONCERTGATE ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CONCERT NIC is online and is prepared to accept route requests from the CONCERT network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1498201</td>
<td>Message</td>
<td>CONCERTGATE OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The CONCERT NIC is offline and cannot accept route requests from the CONCERT network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1498203</td>
<td>Message</td>
<td>SS7 link %1 in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1498204</td>
<td>Message</td>
<td>SS7 link %1 out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>149820B</td>
<td>Message</td>
<td>SS7 linkset %1 unavailable.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>149820C</td>
<td>Message</td>
<td>SS7 linkset %1 available.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1498210</td>
<td>Message</td>
<td>INAP Gateway ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The INAP Gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>INAP Gateway STOPPED. (%1)</td>
<td>Message</td>
<td><strong>INAP Gateway STOPPED. (%1)</strong></td>
</tr>
<tr>
<td>Error</td>
<td>Severity</td>
<td>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.</td>
</tr>
<tr>
<td>Raise</td>
<td>Type</td>
<td>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 Support Center should be alerted to investigate and correct the problem.</td>
</tr>
<tr>
<td>14B0017</td>
<td>Message</td>
<td>Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.</td>
</tr>
<tr>
<td>Error</td>
<td>Severity</td>
<td>TELFORT NIC was unable to connect to the GATEWAY on the TELFORT network.</td>
</tr>
<tr>
<td>Raise</td>
<td>Type</td>
<td>Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity would allow for connection</td>
</tr>
<tr>
<td>14B8009</td>
<td>Message</td>
<td>GATEWAY [%1] is now accessible.</td>
</tr>
<tr>
<td>Informational</td>
<td>Severity</td>
<td>The TELFORT NIC has established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.</td>
</tr>
<tr>
<td>Clear</td>
<td>Type</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14B800A</td>
<td>Message</td>
<td>GATEWAY [%1] is no longer accessible.</td>
</tr>
<tr>
<td>Error</td>
<td>Severity</td>
<td>The TELFORT NIC has disconnected the communication sessions established with the indicated GATEWAY.</td>
</tr>
<tr>
<td>Raise</td>
<td>Type</td>
<td>TELFORT network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>14B800C</td>
<td>Message</td>
<td>GATEWAY [%1] is not accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Although connected, the TELFORT NIC cannot establish a session with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>TELFORT network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>14B8200</td>
<td>Message</td>
<td>TELFORT NIC Routing Client is ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TELFORT NIC is online and is prepared to accept route requests from the TELFORT network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14B8201</td>
<td>Message</td>
<td>TELFORT NIC Routing Client is OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TELFORT NIC is offline and cannot accept route requests from the TELFORT network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14B8203</td>
<td>Message</td>
<td>SS7 link %1 in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>
### Message ID 14B8204

**Property** | **Value**
--- | ---
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 Support Center.

### Message ID 14B820B

**Property** | **Value**
--- | ---
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 Support Center.

### Message ID 14B820C

**Property** | **Value**
--- | ---
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.

### Message ID 14B8210

**Property** | **Value**
--- | ---
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.
<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>14B8211</td>
<td>Message</td>
<td>INAP Gateway STOPPED. (%1)</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 Support Center should be alerted to investigate and correct the problem.</td>
</tr>
<tr>
<td>14B8310</td>
<td>Message</td>
<td>SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14B8311</td>
<td>Message</td>
<td>SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>14B8312</td>
<td>Message</td>
<td>SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>14B8313</td>
<td>Message</td>
<td>SS7 linkset available (Gateway PC=%1, Linkset RPC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14C0017</td>
<td>Message</td>
<td>Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>BT-V2 INAP NIC was unable to connect to the GATEWAY on the INAP network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity would allow for connection</td>
</tr>
<tr>
<td>14C8009</td>
<td>Message</td>
<td>GATEWAY [%1] is now accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The BT-V2 INAP NIC has established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>14C800A</td>
<td>Message</td>
<td>GATEWAY [%1] is no longer accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The BT-V2 INAP NIC has disconnected the communication sessions established with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>INAP network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>14C800C</td>
<td>Message</td>
<td>GATEWAY [%1] is not accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Although connected, the BT-V2 INAP NIC cannot establish a session with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>INAP network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>14C8200</td>
<td>Message</td>
<td>BT-V2 NIC Routing Client is ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The BT-V2 INAP NIC is online and is prepared to accept route requests from the INAP network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14C8201</td>
<td>Message</td>
<td>BT-V2 NIC Routing Client is OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The BT-V2 INAP NIC is offline and cannot accept route requests from the INAP network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14C8203</td>
<td>Message</td>
<td>SS7 link %1 in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>14C8204</td>
<td>Message</td>
<td>SS7 link %1 out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Action</td>
<td></td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>14C820B</td>
<td>Message</td>
<td>SS7 linkset %1 unavailable.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Action</td>
<td></td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>14C820C</td>
<td>Message</td>
<td>SS7 linkset %1 available.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Action</td>
<td></td>
<td>No action is required.</td>
</tr>
<tr>
<td>14C8210</td>
<td>Message</td>
<td>INAP Gateway ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td>The INAP Gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.</td>
</tr>
<tr>
<td>Action</td>
<td></td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>14C8211</td>
<td>Message</td>
<td>INAP Gateway STOPPED. (%1)</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 Support Center should be alerted to investigate and correct the problem.</td>
</tr>
<tr>
<td>14C8310</td>
<td>Message</td>
<td>SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14C8311</td>
<td>Message</td>
<td>SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>14C8312</td>
<td>Message</td>
<td>SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>14C8313</td>
<td>Message</td>
<td>SS7 linkset available (Gateway PC=%1, Linkset RPC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14D0017</td>
<td>Message</td>
<td>Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>TIM NIC was unable to connect to the GATEWAY on the INAP network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity would allow for connection</td>
</tr>
<tr>
<td>14D8009</td>
<td>Message</td>
<td>GATEWAY [%1] is now accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIM NIC has established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>14D800A</td>
<td>Message</td>
<td>GATEWAY [%1] is no longer accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIM NIC has disconnected the communication sessions established with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>INAP network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>14D800C</td>
<td>Message</td>
<td>GATEWAY [%1] is not accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Although connected, the TIM NIC cannot establish a session with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>INAP network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>14D8200</td>
<td>Message</td>
<td>TIM NIC Routing Client is ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIM NIC is online and is prepared to accept route requests from the INAP network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14D8201</td>
<td>Message</td>
<td>TIM NIC Routing Client is OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIM NIC is offline and cannot accept route requests from the INAP network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14D8203</td>
<td>Message</td>
<td>SS7 link %1 in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>14D8204</td>
<td>Message</td>
<td>SS7 link %1 out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>14D820B</td>
<td>Message</td>
<td>SS7 linkset %1 unavailable.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>14D820C</td>
<td>Message</td>
<td>SS7 linkset %1 available.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14D8210</td>
<td>Message</td>
<td>INAP Gateway ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The INAP Gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>14D8211</td>
<td>Message</td>
<td>INAP Gateway STOPPED. (%1)</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 Support Center should be alerted to investigate and correct the problem.</td>
</tr>
<tr>
<td>14D8310</td>
<td>Message</td>
<td>SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14D8311</td>
<td>Message</td>
<td>SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>14D8312</td>
<td>Message</td>
<td>SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>14D8313</td>
<td>Message</td>
<td>SS7 linkset available (Gateway PC=%1, Linkset RPC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14D8314</td>
<td>Message</td>
<td>SCTP connection is down (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14D8315</td>
<td>Message</td>
<td>ASP is Down (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>14D8316</td>
<td>Message</td>
<td>ASP is Inactive (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14D8317</td>
<td>Message</td>
<td>ASP is Active (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The ASP is Active. Calls can be processed through this connection.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14E0007</td>
<td>Message</td>
<td>Session [%1] closed for reason '%2' by client '%3'.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The client has terminated a communication session with the GKTMP NIC.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14E0008</td>
<td>Message</td>
<td>Session for Client[%1] status[%2] connected to Client %3.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>GKTMP NIC Successfully established a connection with the client.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14E0012</td>
<td>Message</td>
<td>GKTMP NIC ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The GKTMP NIC is online and is prepared to accept route requests from its clients.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>14E0013</td>
<td>Message</td>
<td>GKTMPGATE OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The GKTMP NIC is offline and cannot accept route requests from clients.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14F0017</td>
<td>Message</td>
<td>Session for GATEWAY[%1] Connect FAILED to SS7 GATEWAY at Port %2 at Address %3.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>SS7 IN NIC was unable to connect to the SS7 GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Confirm SS7 GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity would allow for connection</td>
</tr>
<tr>
<td>14F8009</td>
<td>Message</td>
<td>SS7 GATEWAY [%1] is now accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The SS7 IN NIC has established a communication session with the indicated SS7 GATEWAY. This indicates that network connectivity exists to the indicated SS7 GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14F800A</td>
<td>Message</td>
<td>SS7 GATEWAY [%1] is no longer accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The SS7 IN NIC has disconnected the communication sessions established with the indicated SS7 GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>SS7 network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>14F800C</td>
<td>Message</td>
<td>SS7 GATEWAY [%1] is not accessible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Although connected, the SS7 IN NIC cannot establish a session with the indicated GATEWAY.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>SS7 network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>14F8102</td>
<td>Message</td>
<td>SS7 link %1 in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14F8103</td>
<td>Message</td>
<td>SS7 link %1 out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now out of service. This is most likely due</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to a circuit problem between the SS7 Gateway and the adjacent signaling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>point to which this link connects. Equipment problems are also a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>possible cause. Because each link typically belongs to a linkset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>containing two or more links, connectivity between the SS7 Gateway</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and the adjacent signaling point to which this link connects.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Because each link typically belongs to a linkset containing two or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>more links, connectivity between the SS7 Gateway and the adjacent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>signaling point to which the linkset connects.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>14F810A</td>
<td>Message</td>
<td>SS7 linkset %1 unavailable.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 linkset is now unavailable. This means that no</td>
</tr>
<tr>
<td></td>
<td></td>
<td>links in that linkset are operational. Consequently, communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>has failed between the SS7 Gateway and the adjacent signaling point</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to which the linkset connects.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>14F810B</td>
<td>Message</td>
<td>SS7 linkset %1 available.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 linkset is now available. At least one link in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>linkset is operational, although others may still be down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communication between the SS7 Gateway and the adjacent signaling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>point to which the linkset connects has been restored.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>14F8114</td>
<td>Message</td>
<td>SS7 link %1 of linkset %2 is in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14F8115</td>
<td>Message</td>
<td>SS7 link %1 of linkset %2 is out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>14F8310</td>
<td>Message</td>
<td>SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14F8311</td>
<td>Message</td>
<td>SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>14F8312</td>
<td>Message</td>
<td>SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Contact the Support Center.</td>
</tr>
<tr>
<td>14F8313</td>
<td>Message</td>
<td>SS7 linkset available (Gateway PC=%1, Linkset RPC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14F8314</td>
<td>Message</td>
<td>SCTP connection is down (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14F8315</td>
<td>Message</td>
<td>ASP is Down (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>14F8316</td>
<td>Message</td>
<td>ASP is Inactive (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>14F8317</td>
<td>Message</td>
<td>ASP is Active (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The ASP is Active. Calls can be processed through this connection.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1504001</td>
<td>Message</td>
<td>The NTL NIC received an invalid label %1 from the router for the call(tid=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Application Error</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NTL NIC received an invalid label from the router. Check the label format and size.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check labels in the label table for invalid labels.</td>
</tr>
<tr>
<td>1508006</td>
<td>Message</td>
<td>Starting NTL network communications.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The network communication layer of the NTL NIC is starting operation.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1508007</td>
<td>Message</td>
<td>Stopping NTL network communications.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The network communication layer of the NTL NIC is halting operation.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1508009</td>
<td>Message</td>
<td>Starting a NTL communication channel (%1) with CE '%4:%2' .</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A communication channel of the NTL NIC is starting operation.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>150800A</td>
<td>Message</td>
<td>Stopping the NTL communication channel (%1) to CE '%4:%2' .</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A communication channel of the NTL NIC is halting operation.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>150800B</td>
<td>Message</td>
<td>Closing the NTL communication channel (%1) by CE '%4:%2' .</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A communication channel of the NTL NIC is closed by the SCP.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1520017</td>
<td>Message</td>
<td>Session for Gateway[%1] Connect FAILED to Gateway at Port %2 at Address %3.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>NIC unable to connect to the Gateway on the SS7 network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Confirm Gateway is available, configuration of IP address and Port are correct, and network connectivity allows for connection.</td>
</tr>
<tr>
<td>1528009</td>
<td>Message</td>
<td>Gateway[%1] is now accessible (GSP open response accepted).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NIC has established a communication session with the indicated Gateway. This indicates that network connectivity exists to the indicated Gateway.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>152800A</td>
<td>Message</td>
<td>Gateway[%1] is no longer accessible (GSP session closed).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NIC has disconnected the communication sessions established with the indicated Gateway.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>SS7 network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>152800C</td>
<td>Message</td>
<td>Gateway[%1] not accessible (no GSP open response returned); retrying...</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Although connected, the NIC cannot establish a session with the indicated Gateway.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>SS7 network support should be contacted regarding this problem.</td>
</tr>
<tr>
<td>1528200</td>
<td>Message</td>
<td>AT&amp;T Routing Client is ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NIC is online and is prepared to accept route requests from the SS7 network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1528201</td>
<td>Message</td>
<td>AT&amp;T Routing Client is OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The NIC is offline and cannot accept route requests from the SS7 network.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1528301</td>
<td>Message</td>
<td>SS7 link %1 of linkset %2 is in service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1528302</td>
<td>Message</td>
<td>SS7 link %1 of linkset %2 is out of service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Occasional brief outages of a single link 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&amp;T Advanced Features Service Center (AFSC) at 800-621-6901. Ask to speak to an ICP technician.</td>
</tr>
<tr>
<td>1528309</td>
<td>Message</td>
<td>SS7 linkset %1 unavailable.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 linkset to the SS7 network is now in a non-working state. This means that all links (normally one, but possibly more) between the NIC and a particular Signal Transfer Point (STP) in the SS7 network are not operational. This is most likely due to a circuit problem in either the Local Exchange Carrier or in the SS7 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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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&amp;T Advanced Features Services Center (AFDSC) at 800-621-6901. Ask to speak to an ICP technician.</td>
</tr>
<tr>
<td>152830A</td>
<td>Message</td>
<td>SS7 linkset %1 available.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1528310</td>
<td>Message</td>
<td>SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1528311</td>
<td>Message</td>
<td>SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 link is now aligned and in service.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1528312</td>
<td>Message</td>
<td>SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The specified SS7 linkset to the SS7 network is now in a non-working state. This means that all links (normally one, but possibly more) between the NIC and a particular Signal Transfer Point (STP) in the SS7 network are not operational. This is most likely due to a circuit problem in either the Local Exchange Carrier or in the SS7 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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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 ATtheT Advanced Features Services Center (AFDSC) at 800-621-6901. Ask to speak to an ICP technician.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1528313</td>
<td>Message</td>
<td>SS7 linkset available (Gateway PC=%1, Linkset RFC=%2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1528314</td>
<td>Message</td>
<td>SCTP connection is down (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1528315</td>
<td>Message</td>
<td>ASP is Down (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1528316</td>
<td>Message</td>
<td>ASP is Inactive (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1528317</td>
<td>Message</td>
<td>ASP is Active (ConnectionNumber = %1, Remote Entity = %2).</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The ASP is Active. Calls can be processed through this connection.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1528400</td>
<td>Message</td>
<td>SS7 Gateway ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The SS7 Gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1528401</td>
<td>Message</td>
<td>SS7 Gateway STOPPED. (%1)</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The SS7 Gateway has stopped operation due to the specified error code. The ICP 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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>This event can be caused by a transient problem which may be automatically corrected as indicated by a 'SS7 Gateway ONLINE' event. If the problem persists for more than three minutes, the Support Center should be alerted to investigate and correct the problem.</td>
</tr>
</tbody>
</table>
# ICM Hosted Events

Table 80:

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>12C8200</td>
<td>Message</td>
<td>Communications to CICR %1 is ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>At least one link with this CICR is now open and carrying traffic.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12C8201</td>
<td>Message</td>
<td>Communications to CICR %1 is OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>For some reason all the links to the CICR have terminated or were</td>
</tr>
<tr>
<td></td>
<td></td>
<td>never established. If any links were established, there should</td>
</tr>
<tr>
<td></td>
<td></td>
<td>have been messages describing when and why the link or links</td>
</tr>
<tr>
<td></td>
<td></td>
<td>failed. If configured to do so the CIC will continue to attempt to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>open the links.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Determine why communications is not being established which may</td>
</tr>
<tr>
<td></td>
<td></td>
<td>include LAN or WAN configuration or the CICR machine failing.</td>
</tr>
<tr>
<td>12C8202</td>
<td>Message</td>
<td>Link to CICR %1 side %2 is now ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A session with this CICR's side is now open and carrying traffic.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12C8203</td>
<td>Message</td>
<td>Link to CICR %1 side %2 is OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>For some reason the link to the CICR has terminated or was never</td>
</tr>
<tr>
<td></td>
<td></td>
<td>established. There is usually an error message preceding this</td>
</tr>
<tr>
<td></td>
<td></td>
<td>message in the log file which gives an explanation for the link</td>
</tr>
<tr>
<td></td>
<td></td>
<td>going down. If configured to do so the CIC will continue to attempt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to open the link.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Determine why the link is not being established which may include</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LAN or WAN configuration.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>12C8204</td>
<td>Message</td>
<td>Configuration for Link to CICR %1 side %2 is now VALID.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The configuration for the connection between the Network ICM and the CICR's side is now valid.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12C8205</td>
<td>Message</td>
<td>Configuration for Link to CICR %1 side %2 is VOID.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The configuration for the connection between the Network ICM and the CICR's side is not valid. This is usually due to either the IP Address or Instance Number being invalid. However, if a link or number of links were deconfigured and reconfigured before the original links could be closed, the system would not be able to keep multiple copies of the configuration and hence would produce this error. If the latter problem occurs, simply reconfigure the link or links after they have had time to close.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check the IP Address, Instance Number, and Preferred Side in the ICM Configuration for the Customer ICM and update the central data base.</td>
</tr>
<tr>
<td>12C8206</td>
<td>Message</td>
<td>Link from CIC Side A to CICR %1 Side %2 is now ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A session with this CICR's side is now open and carrying traffic.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12C8207</td>
<td>Message</td>
<td>Link from CIC Side A to CICR %1 Side %2 is OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>For some reason the link to the CICR has terminated or was never established. There is usually an error message preceding this message in the log file which gives an explanation for the link going down. If configured to do so the CIC will continue to attempt to open the link.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Determine why the link is not being established which may include LAN or WAN configuration.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>12C8208</td>
<td>Message</td>
<td>Configuration for Link between CIC Side A and CICR %1 Side %2 is now VALID.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The configuration for the connection between the Network ICM and the CICR's side is now valid.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12C8209</td>
<td>Message</td>
<td>Configuration for Link between CIC Side A and CICR %1 Side %2 is VOID.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The configuration for the connection between the Network ICM and the CICR's side is not valid. This is usually due to either the IP Address or Instance Number being invalid. However, if a link or number of links were deconfigured and reconfigured before the original links could be closed, the system would not be able to keep multiple copies of the configuration and hence would produce this error. If the latter problem occurs, simply reconfigure the link or links after they have had time to close.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check the IP Address, Instance Number, and Preferred Side in the ICM Configuration for the Customer ICM and update the central database.</td>
</tr>
<tr>
<td>12C8210</td>
<td>Message</td>
<td>Link from CIC Side B to CICR %1 Side %2 is now ONLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A session with this CICR's side is now open and carrying traffic.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12C8211</td>
<td>Message</td>
<td>Link from CIC Side B to CICR %1 Side %2 is OFFLINE.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>For some reason the link to the CICR has terminated or was never established. There is usually an error message preceding this message in the log file which gives an explanation for the link going down. If configured to do so the CIC will continue to attempt to open the link.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Determine why the link is not being established which may include LAN or WAN configuration.</td>
</tr>
</tbody>
</table>
### ValuePropertyMessage ID

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>12C8212</td>
<td>Message</td>
<td>Configuration for Link between CIC Side B and CICR %1 Side %2 is now VALID.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The configuration for the connection between the Network ICM and the CICR’s side is now valid.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>12C8213</td>
<td>Message</td>
<td>Configuration for Link between CIC Side B and CICR %1 Side %2 is VOID.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The configuration for the connection between the Network ICM and the CICR’s side is not valid. This is usually due to either the IP Address or Instance Number being invalid. However, if a link or number of links were deconfigured and reconfigured before the original links could be closed, the system would not be able to keep multiple copies of the configuration and hence would produce this error. If the latter problem occurs, simply reconfigure the link or links after they have had time to close.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check the IP Address, Instance Number, and Preferred Side in the ICM Configuration for the Customer ICM and update the central data base.</td>
</tr>
</tbody>
</table>

### Symposium/AAS Events

#### Table 81:

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1530002</td>
<td>Message</td>
<td>A required parameter is invalid.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>One or more of the required parameters are invalid.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Internal error. Contact tech support.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1530003</td>
<td>Message</td>
<td>The maximum SEI event queue size was exceeded.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The maximum SEI event queue size was exceeded.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Change the configuration in the registry (see Troubleshooting Guide) to allow for a greater queue size.</td>
</tr>
<tr>
<td>1530015</td>
<td>Message</td>
<td>One or more ICM/AW connection parameters are null or empty.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>One or more required ICM/AW connection parameters are null or empty.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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.</td>
</tr>
<tr>
<td>1530017</td>
<td>Message</td>
<td>Fatal connection error to ICM/AW.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>All retry and failover attempts to the ICM AW('s) have failed.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>See the AAS Installation and Troubleshooting Guide for information on correcting connection errors.</td>
</tr>
<tr>
<td>1530018</td>
<td>Message</td>
<td>ICM/AW authentication failed.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>AAS is unable to log into the ICM/AW because the login authentication failed.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1530019</td>
<td>Message</td>
<td>Unable to retrieve a PG Name from the Peripheral table.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Unable to retrieve a PG Name from the Peripheral table.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Make sure a PG Name is configured for the peripheral that is set up for AAS.</td>
</tr>
<tr>
<td>153001A</td>
<td>Message</td>
<td>Error adding record to ICM/AW.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>153001B</td>
<td>Message</td>
<td>Error deleting record from ICM/AW.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>AAS was unable to delete a record from ICM/AW. A possible reason is that the ICM/AW is out of sync with Symposium.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>153001C</td>
<td>Message</td>
<td>Error updating record in ICM/AW.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>AAS was unable to update a record in ICM/AW. A possible reason is that the ICM/AW is out of sync with Symposium.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>153001D</td>
<td>Message</td>
<td>Error performing bulk update of the ICM/AW.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>153001E</td>
<td>Message</td>
<td>Bad ICM/AW operation type used.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A bad ICM/AW operation type was used. Update, delete, insert, and destroy permanently are the only operation types supported.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Internal error. Contact tech support.</td>
</tr>
<tr>
<td>153001F</td>
<td>Message</td>
<td>Lost connection to the ICM/AW.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>AAS lost its connection to the ICM/AW due to an unknown cause.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>AAS should self-correct. If it does not, consult the AAS Installation and Troubleshooting Guide for information on correcting connection errors to ICM.</td>
</tr>
<tr>
<td>1530020</td>
<td>Message</td>
<td>Error retrieving records from the ICM/AW.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>AAS was unable to retrieve records from the ICM/AW. A possible reason is that the ICM/AW is out of sync with Symposium.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1530021</td>
<td>Message</td>
<td>Error retrieving peripheral record from ICM/AW.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>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).</td>
</tr>
<tr>
<td>1530022</td>
<td>Message</td>
<td>Error retrieving skill group from ICM/AW.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>1530023</td>
<td>Message</td>
<td>Agent priority specified is beyond maximum allowed limits.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The agent priority specified was configured with a priority greater than the maximum allowed limit of 48.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Internal error. Contact technical support.</td>
</tr>
<tr>
<td>1530025</td>
<td>Message</td>
<td>An attempt was made to remove an agent from a skill group and either the agent or the skill group does not exist.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>AAS attempted to remove an agent from a skill group and either the agent or the skill group does not exist.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1530026</td>
<td>Message</td>
<td>An attempt was made to remove an agent from a skill group where no such assignment exists.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>An attempt was made to remove an agent from a skill group where no such assignment exists.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Resync ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>1530027</td>
<td>Message</td>
<td>A request was made to add an agent in a bulk operation where no corresponding person exists.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A request was made to add an agent in a bulk operation where no corresponding person exists.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1530033</td>
<td>Message</td>
<td>Config services requested before config info set.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Configuration services were requested before the configuration information was set up.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Internal error. Contact technical support.</td>
</tr>
<tr>
<td>1530034</td>
<td>Message</td>
<td>An unexpected key type was given to the config service.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A configuration parameter for AAS was setup with the wrong key type in the registry.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Recreate the key with the proper type (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1530035</td>
<td>Message</td>
<td>All attempts to connect to Symposium have failed.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>All attempts to connect to Symposium have failed.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Ensure that all the Symposium services are started and running. Check that the Symposium configuration/connection information is correct.</td>
</tr>
<tr>
<td>1530036</td>
<td>Message</td>
<td>Error performing post resync processing.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Check for a broken connection to the ICM or other errors in the log for problems accessing the database.</td>
</tr>
<tr>
<td>1530037</td>
<td>Message</td>
<td>An event was discarded.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>An event was discarded due to a data access exception received from ICM/AW (ConAPI).</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1530038</td>
<td>Message</td>
<td>Registration with SEI server failed.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The registration with SEI server failed.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Ensure the SEI configuration in the registry (see Troubleshooting Guide) is correct.</td>
</tr>
<tr>
<td>1530039</td>
<td>Message</td>
<td>Request for initial SEI events failed.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The request for initial SEI events failed.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Make sure the Symposium services are started and functioning properly.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1530040</td>
<td>Message</td>
<td>AAS failed to establish a connection to SEI.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>AAS failed to establish a connection to SEI.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1530041</td>
<td>Message</td>
<td>The maximum allowable event queue size has been exceeded.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The maximum allowable event queue size has been exceeded even though the ICM/AW appears to be functioning normally. Some causes are a slow network, a slow ICM/AW, or a slow database.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>The problem may be fixed by increasing the value in the AASSEIMaxEventQueueSize registry (see Troubleshooting Guide) setting.</td>
</tr>
<tr>
<td>1530051</td>
<td>Message</td>
<td>Configuration given to MasterSelection is null.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>MasterSelection cannot start because the AAS PG hosts and ports were not configured in the registry.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Correct registry data for AASPG Hosts and Ports (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>1530052</td>
<td>Message</td>
<td>Bad IP address for Side A MasterSelection.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The configuration IP address for the Side A MasterSelection is badly formed or cannot be found.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Correct the AASPGHostA and AASPGPortA configuration data in the registry (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>1530053</td>
<td>Message</td>
<td>Bad IP address for Side B MasterSelection.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The configuration IP address for the Side B MasterSelection is badly formed or cannot be found.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Correct the AASPGHostB and AASPGPortB configuration data in the registry (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>1530054</td>
<td>Message</td>
<td>Null IP address for Side A MasterSelection.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The configuration IP address for the Side A MasterSelection is blank, which is not allowed.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Correct the AASPGHostA and AASPGPortA configuration data in the registry (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>1530055</td>
<td>Message</td>
<td>Null IP address for Side B MasterSelection.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The configuration IP address for the Side B MasterSelection is blank, which is not allowed.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Correct the AASPGHostB and AASPGPortB configuration data in the registry (see Troubleshooting Guide).</td>
</tr>
<tr>
<td>1530056</td>
<td>Message</td>
<td>BindException or SocketException trying to open socket for MasterSelection</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>MasterSelection could not open a socket for communication.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>The network administrator should make sure the Side A and B servers can communicate with each other.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1530057</td>
<td>Message</td>
<td>Due to the max event queue size being exceeded, a resync of Symposium events is being requested.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A Symposium resync is being requested because the maximum event queue size has been exceeded.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>This is most likely due to a configuration error in the registry. Check the registry (see Troubleshooting Guide) and make sure it is correct.</td>
</tr>
<tr>
<td>15301F4</td>
<td>Message</td>
<td>AAS disconnected from the ICM/AW.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>AAS disconnected from the ICM/AW.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>AAS should reset it's connection to ICM. If it doesn't, restart AAS.</td>
</tr>
<tr>
<td>15301F6</td>
<td>Message</td>
<td>Connection to the ICM/AW established.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The connection between AAS and the ICM/AW has been established.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1530235</td>
<td>Message</td>
<td>MasterSelection has been started.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>MasterSelection IP addresses have been checked, a socket opened, and threads started.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>
## Live Data Events (Packaged CCE only)

### Table 82:

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1588000</td>
<td>Message</td>
<td>TIP Server at [%2:%1] has been started</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIP Server has been started.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1588002</td>
<td>Message</td>
<td>TIP Server has been disabled</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIP Server has been disabled.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1588003</td>
<td>Message</td>
<td>TIP Server at [%2:%1] is waiting for client connection</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIP Server is waiting for client connections.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>If condition persists, ensure that Live Data client is running, has connectivity, and correct configuration information to contact this TIP server.</td>
</tr>
<tr>
<td>1588004</td>
<td>Message</td>
<td>TIP Server at [%3:%1] accepted a connection from [%4:%2]</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIP Server has accepted a client connection</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>1588006</td>
<td>Message</td>
<td>TIP Server at [%3:%1] client connection [%4:%2] failed [%5]</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIP Server client connection has failed.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1588007</td>
<td>Message</td>
<td>TIP Server at [%2:%1] has been stopped</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIP Server has been stopped.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
<tr>
<td>1588008</td>
<td>Message</td>
<td>TIP Server at [%5:%1] is above warning memory threshold (%2 MB). Queue will be maintained at %4 will be deleted until memory drops below %3 MB. TIP event loss possible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIP Server has exceeded configured warning memory limits. Oldest TIP events are being deleted before acknowledge received, making event loss possible.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>If condition persists, ensure that Live Data client is running, has connectivity, and correct configuration information to contact this TIP server.</td>
</tr>
<tr>
<td>1588009</td>
<td>Message</td>
<td>TIP Server at [%5:%1] is above critical memory threshold (%2 MB). Queue will be reduced from %4 will be deleted until memory drops below %3 MB. TIP event loss possible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIP Server has exceeded configured critical memory limits. Oldest TIP events are being deleted before acknowledge received, making event loss possible.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>If condition persists, ensure that Live Data client is running, has connectivity, and correct configuration information to contact this TIP server.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>158800A</td>
<td>Message</td>
<td>TIP Server at [%5:%1] is within memory and queue size limits. Current %4 will be kept in queue.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Informational</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Clear</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIP Server is within configured memory limits.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>None</td>
</tr>
<tr>
<td>158800B</td>
<td>Message</td>
<td>TIP Server at [%5:%1] has exceeded maximum %4 will be deleted until queue size is reduced. TIP event loss possible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIP Server has exceeded configured maximum queue size. Oldest TIP events are being deleted before acknowledge received, making event loss possible.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>If condition persists, ensure that Live Data client is running, has connectivity, and correct configuration information to contact this TIP server.</td>
</tr>
<tr>
<td>158800C</td>
<td>Message</td>
<td>TIP Server at [%5:%1] has exceeded Warning memory threshold (%2 MB), but Queue is below minimum size (%3). Queue may grow at %4 will be kept in queue.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Monitor process memory usage and take appropriate action if memory overflow is imminent.</td>
</tr>
<tr>
<td>158800D</td>
<td>Message</td>
<td>TIP Server at [%5:%1] has exceeded Critical memory threshold (%2 MB), but Queue is below minimum size (%3). Queue may grow at %4 will be kept in queue.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Monitor process memory usage and take appropriate action if memory overflow is imminent.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>158800E</td>
<td>Message</td>
<td>TIP Server at [%5:%1] has exceeded critical memory threshold (%2 MB), maintain Queue at minimum %4 will be deleted until memory drops below %3 MB. TIP event loss possible.</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Raise</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>The TIP Server has exceeded configured critical memory limits. Oldest TIP events are being deleted before acknowledge received, making event loss possible.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Monitor process memory usage and take appropriate action if memory overflow is imminent.</td>
</tr>
<tr>
<td>12A0003</td>
<td>Message</td>
<td>HeartBeat Event for %1</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Periodic message to indicate MDS is in service and that the event stream is active.</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>