Serviceability Best Practices Guide for Cisco Unified ICM/Unified CCE & Unified CCH

Release 9.0

Last Updated: August 30, 2012

Corporate 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: 408 526-4100

Serviceability Best Practices Guide for Cisco Unified ICM/Unified CCE & Unified CCH for Release 8.5(1)

Table of Contents

List of Tables

List of Figures

1 Introduction

The Serviceability Best Practices Guide is intended to provide information to effectively monitor and manage Cisco Unified Contact Center Enterprise (Unified CCE), Cisco Unified Contact Center Hosted (Unified CCH), Cisco Unified Intelligent Contact Management Enterprise (Unified ICME) and Cisco Unified Intelligent Management Hosted (Unified ICMH).

1.1 Target Audience

The target audience for this document is system administrators who monitor and manage Unified CCE/Unified CCH and Unified ICME/Unified ICMH.

1.2 Document Intent and Focus

The intent of this document is to provide the reader (presumably one who does not necessarily possess extensive, detailed knowledge of the use of the Unified ICM or Unified CCE) with sufficient information to understand the product from a management perspective, and to describe in detail the capabilities of the management interfaces and features. The hope is that the reader can then formulate a management and monitoring strategy or easily integrate the management of the Unified ICM/Unified CCE into an existing network management infrastructure.

The focus of this document is the Unified CCE. The vast majority of the content and serviceability features are supported by (and the vast majority of the content applies to) Unified ICME management as well. Situations where certain content is specific only to one product or the other, is noted.

1.3 Product Names

Some of the product names and other terminology have changed over time. Some of the supporting documentation was not updated to reflect the new names. In some cases, user interfaces and splash screens must be modified to reflect current release product names.

Table 1-1: Product Names

Current Name	Previous Name	Also Known As	Notes
Cisco Unified Contact Center Enterprise (Unified CCE)	IP Contact Center Enterprise Edition (IPCC/E)	Classic IPCC	
Cisco Unified Contact Center Hosted (Unified CCH)	IP Contact Center Hosted Edition (IPCC/H)	Hosted IPCC	
Outbound Option	Blended Agent		User Interface and some documentation may still refer to this as Blended Agent.
Cisco Unified Intelligent Contact Management Enterprise (Unified ICME)	Intelligent Contact Management Enterprise Edition (ICM/E)	Intelligent Call Router (ICR)	

Current Name	Previous Name	Also Known As	Notes
Cisco Unified Intelligent Contact Management Hosted (Unified ICMH)	Intelligent Contact Management Hosted Edition (ICM/H)		

2 Product Architecture

The following section provides an overview of the Cisco Unified Contact Center (Unified CC) Architecture.

2.1 Overview—Cisco Unified Contact Center

The 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 multi-channel automatic call distributor (ACD) functionality with IP telephony in a unified solution, enabling customers to rapidly deploy a distributed contact center infrastructure.

Unified Contact Center 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 customer needs based on real-time conditions (such as agent skills, availability, and queue lengths) continuously gathered from various contact center components

The Unified Contact Center enables customers 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.

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

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

The Unified ICM platform was originally designed to route calls between various nodes in the TDM telephone network. It is designed with an emphasis on reliability and flexibility. All processing in these components is message based. The processing of each message is determined entirely by the content of the message, and the current state of the process. 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 the Unified Contact Center is its redundancy strategy. The components that contain centralized state are run in duplex, in that two of these components work in lockstep to ensure redundancy and immediate recovery from a (single point of failure) fault.

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

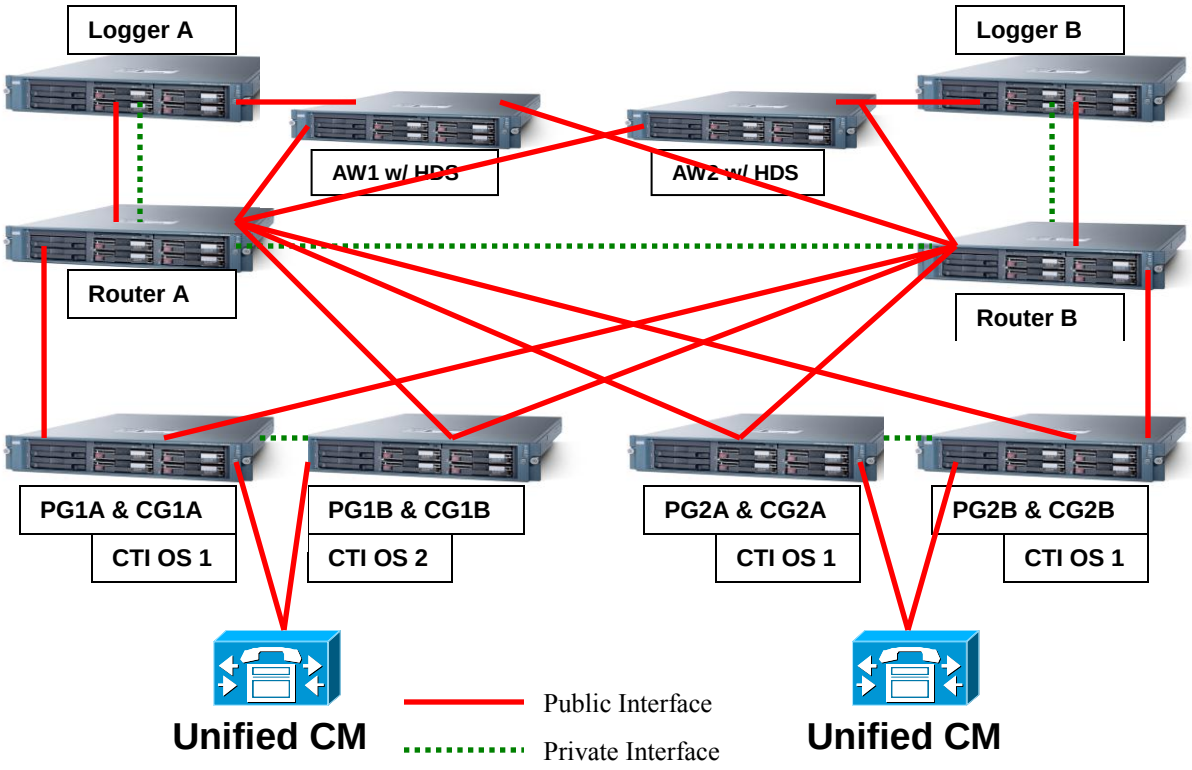


Figure 1: Unified CCE Architecture

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

1. Router: Make the routing decisions – select a peripheral or agent to receive an inbound contact (voice call, email, chat and so on).
2. Logger: Store (and replicate) all configuration, real-time and historical data.
3. Peripheral Gateway: Act as a gateway to a peripheral device – an IP PBX or an Interactive Voice Response (IVR) unit – as well as a CTI gateway linking agent desktops.
4. Administration Workstation: A server implementation that provides a copy of 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).

2.2 Router

The Router is the brain of the Unified CCE. The 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.

2.2.1 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.

2.3 Logger

The 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 as well as summary messages that the PGs compute and send through the Router. Examples of these are half-hour summaries (how many calls were received during a given period).

The Logger uses a synchronization process that is a little different than the Router. The messages coming to the Logger are sent only from the corresponding Router. Side A Router sends messages only to the Side A Logger. Side B Router sends messages only to the Side B Logger. Because the Routers are running in lockstep, it is guaranteed that while messages are flowing they are the same messages; however, recovery happens directly from Logger to Logger, using bulk database copy algorithms for efficiency.

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

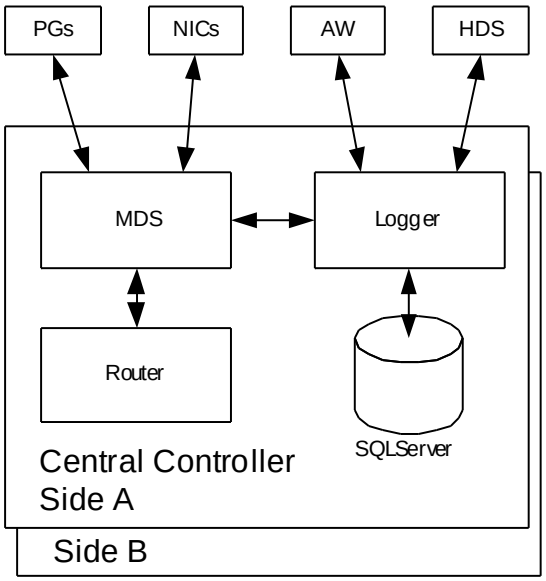


Figure 2: Central Controller Architecture

2.4 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 the 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 the 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 the Unified CCE. The new PG coordinates these calls and makes that call look like a single call. This is what happens on a traditional TDM ACD, where the ACD also has a queue point.

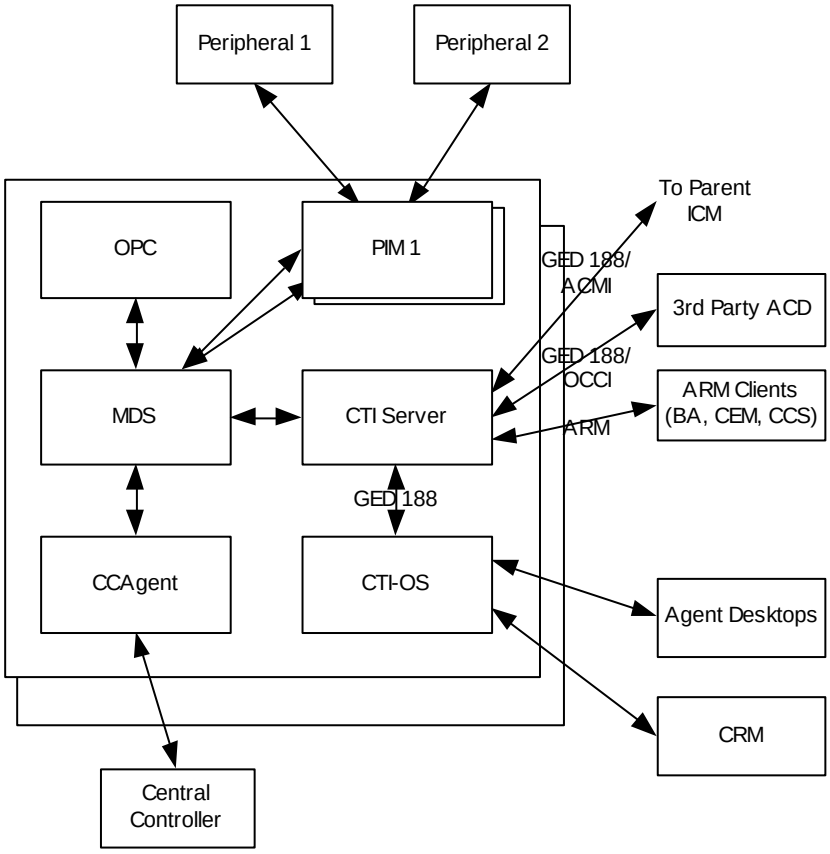


Figure 3: Peripheral Gateway Architecture

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

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

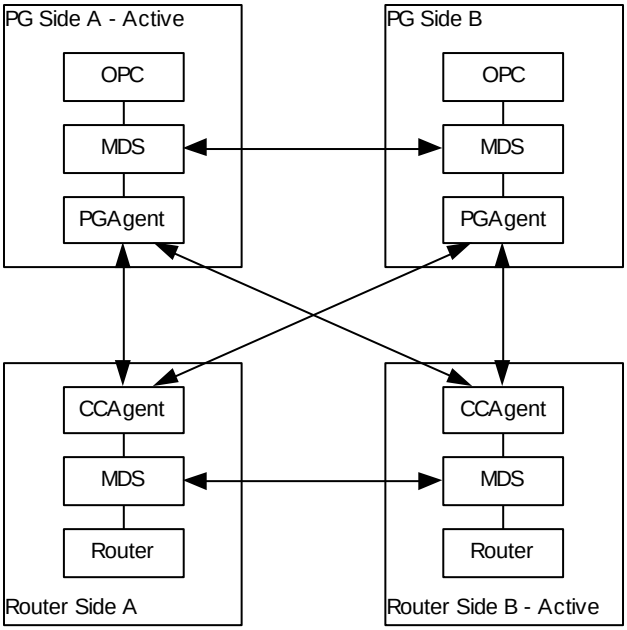


Figure 4: DMP Flows

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

2.4.1 Open Peripheral Controller

The Open Peripheral Controller (OPC) computes and maintains the state of agents on the PG, reporting that state to the Router, knowing when a call needs to request instructions from the Router, and performing 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.

2.4.2 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.

2.4.2.1 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 the Unified CM through the JTAPI Gateway.

2.4.2.2 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.

2.4.2.3 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.

2.4.2.4 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.

2.4.3 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.

2.4.4 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 has been used as a direct CTI connection to agent desktops or third-party desktops. This use has been deprecated.

GED-188 helps to make the details of individual peripherals hidden, but does not fully complete the job. The messages sent from a CTI Server connected to an Aspect PG are different than 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 – this is the client of choice for agent and supervisor desktops, as well as 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 multi-channel (e-mail and web collaboration) applications as well as 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, as well as to take control of certain incoming calls and route them itself. This variance of GED-188 is known as ACMI.

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

2.4.5 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.

2.4.6 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
- Enterprise 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 CTI OS 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 2-1: CAD Services and Executables

Service Name	Executable Name
Cisco Browser and IP Phone Agent Service	IPPASvr.exe
Cisco Chat Service	FCCServer.exe
Cisco Enterprise Service	CTI Storage Server.exe
Cisco LDAP Monitor Service	LDAPmonSvr.exe
Cisco Licensing and Resource Manager Service	LRMServer.exe
Cisco Recording & Playback Service	RPServer.exe
Cisco Recording and Statistics Service	FCRasSvr.exe
Cisco Sync Service	DirAccessSynSvr.exe
Cisco VoIP Monitor Service	FCVoIPMonSvr.exe

Directory Replication Service	slurpd.exe
Directory Services	slapd.exe
Tomcat Service	tomcat5.exe

For more information about administering CAD services, see the *Cisco CAD Service Information Manual*.

2.5 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.

2.5.1 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, which are used to provide a GUI to update the configuration, and the Configuration Management Server (CMS) process, which is used to provide the Configuration API (ConAPI).

Processes that connect to ConAPI are the multi-channel 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 – so that if a failure occurs on the primary link, the secondary is utilized to recover from the failure and restore 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); this type includes only configuration data needed for historical reporting purposes.

2.5.2 Configuration Updates

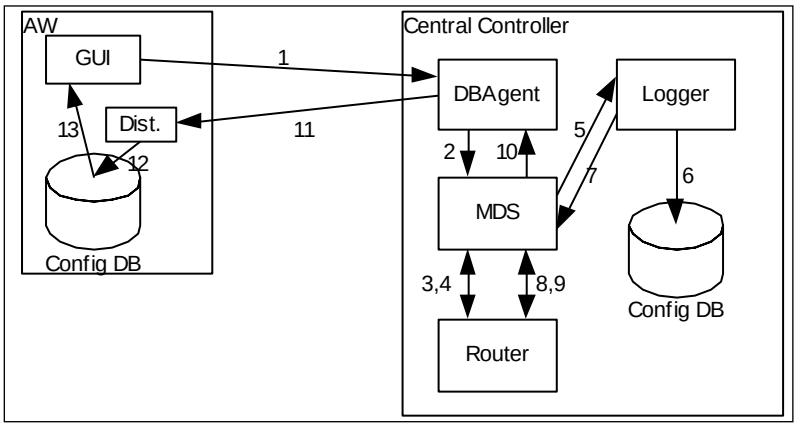


Figure 5: Configuration System Message Flow

Figure 5 illustrates how a configuration update may happen in the 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 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 of its clients (DBAgent, PGs, etc) (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).

2.6 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.

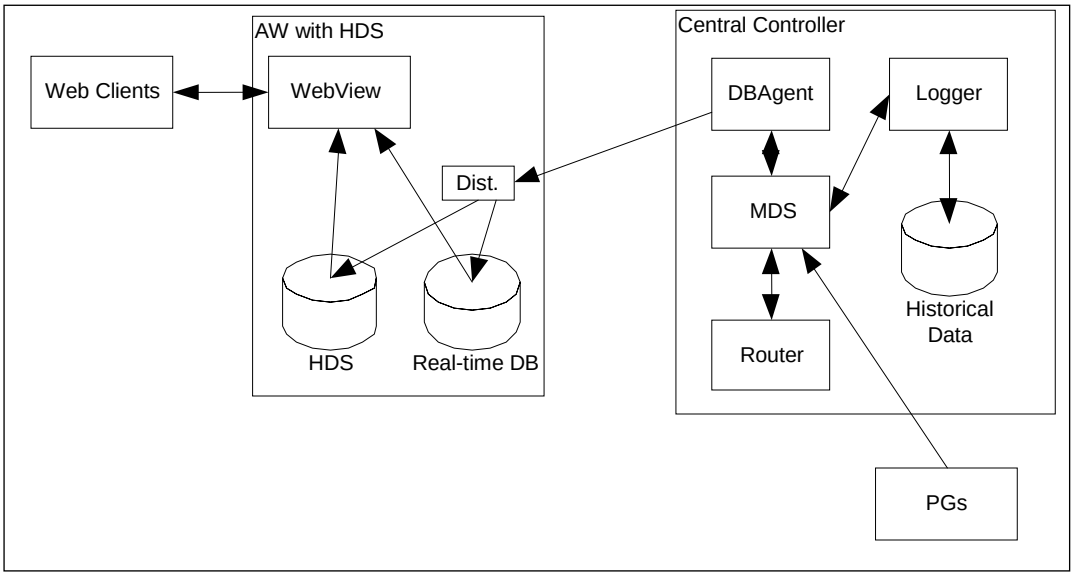


Figure 6: Reporting Architecture

Note: In the preceding diagram, the "WebView" component shown may be either the WebView server component (which may be coresident on the AW/HDS or standalone on its own server) or the Unified Intelligence Center component.

2.6.1 Historical Data Server

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

There are three types of HDSs:

1. **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/medium deployments but only one per Logger side in a large deployment (presumably with multiple AW-HDS servers).
2. **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.

3. **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 in conjunction with multiple AW-HDS servers. There may be a maximum of one HDS-DDS per Logger side (presumably with multiple AW-HDS servers).

2.6.2 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
- Report scheduler
- Detailed security levels and LDAP/local database authentication
- Import and export of report XML files
- Export of grid reports to Microsoft Excel

- Multiple languages
- Clustered deployment
- Management support through Simple Network Management Protocol (SNMP), Java Management Extensions (JMX), and Cisco Analysis Manager

2.6.2.1 Unified Intelligence Center Standard Deployment Model

The Unified Intelligence Center deployment with the Unified CCE utilizes 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 better throughput in data extracted and ensures faster response times for reports, especially real-time reports with repeated refresh intervals.

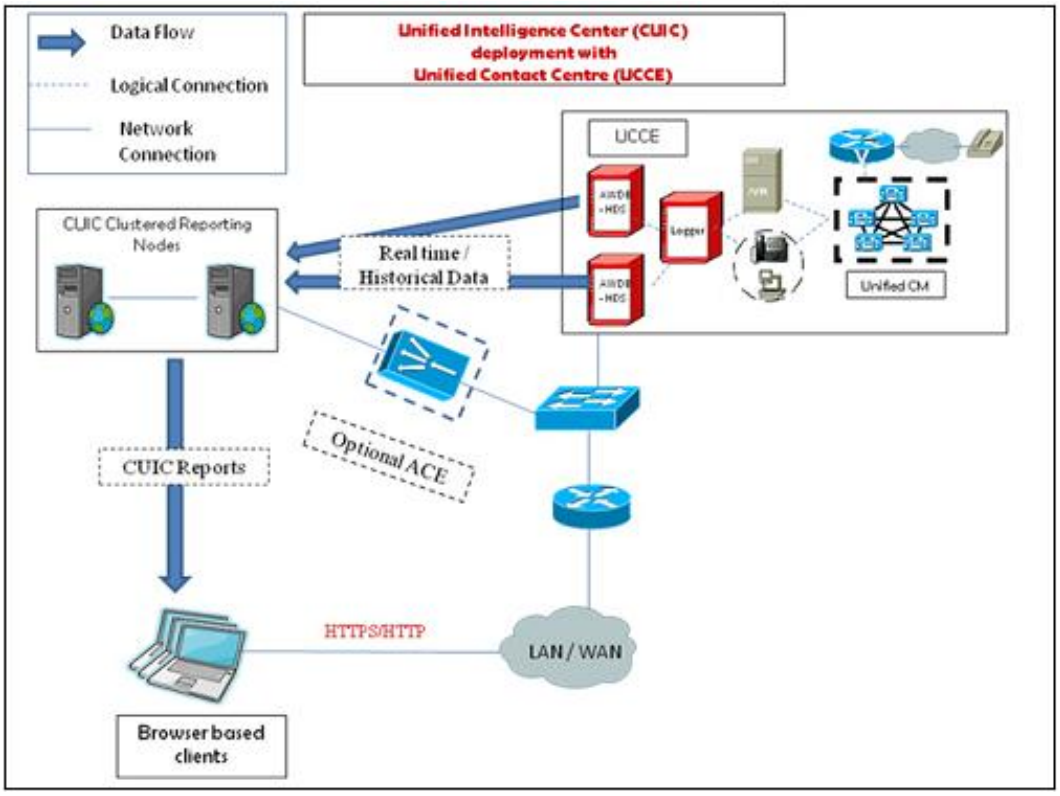


Figure 7: Unified Intelligence Center Standard Deployment

2.6.2.2 Unified Intelligence Center Scaled Deployment Model

You can deploy the Unified Intelligence Center as the reporting solution with Unified CCE deployments that scale over WAN networks. In these deployments, the Unified Intelligence Center is deployed locally with one section/data center of the scaled Unified CCE

deployment and can access the local AW-HDS over the Local Area Network (LAN), as well as the remote AW-HDS, which is deployed along with the remote section of the Unified CCE over the Wide Area Network (WAN).

You can deploy other data sources, such as the Cisco Unified Customer Voice Portal, along with the Unified CCE. Firewall considerations when you deploy over the WAN are applicable to the data source servers and appropriate ports as described in Cisco Unified Intelligence Center Solution Reference Network Design (SRND), should be opened, depending on the remote database configuration.

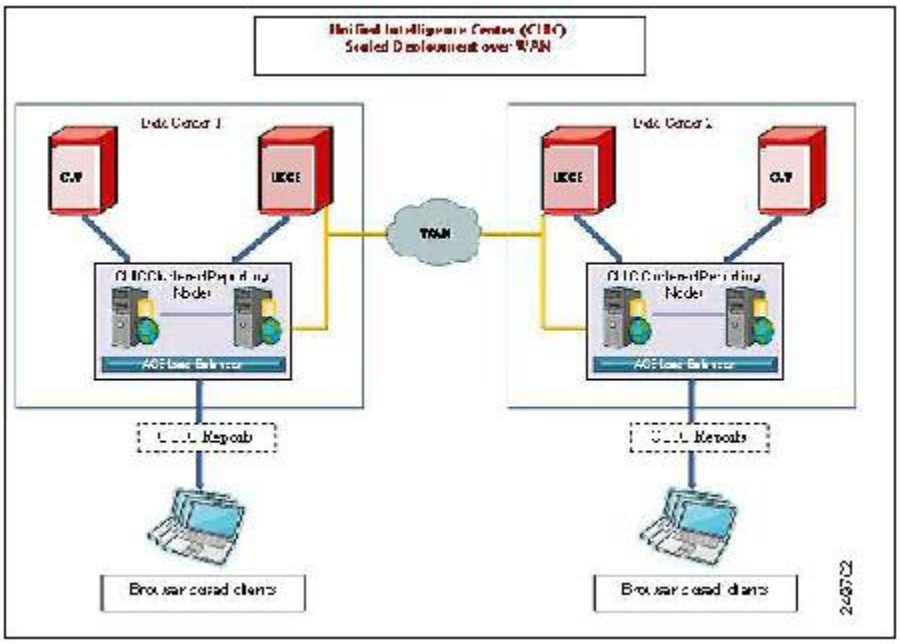


Figure 8: CUIC Scaled Deployment

2.6.3 Unified Contact Center Management Portal

The 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. The Unified CCMP consists of four components:

- The **Database Server** component, which utilizes 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 as well as 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.

The 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. The 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 Unified CCMP system architecture is shown below. The top half of the diagram is a traditional three tier application. This 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*.

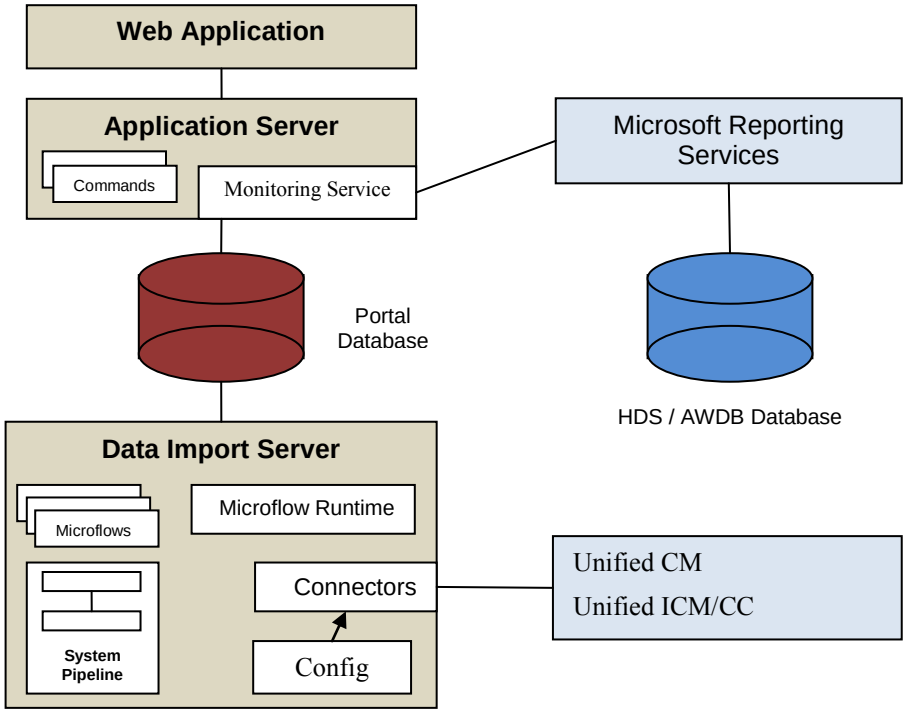


Figure 9: Unified CCMP Architecture

Web Application

The user interface to the 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) and so 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

The Unified CCMP utilizes Microsoft Reporting Services technology for generating reports. Microsoft Reporting Services is an integral part of SQL Server Enterprise Edition. The 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 the Unified CCMP. The Data Import Server component imports the data used in the Unified CCMP. It is designed to handle high volume data (facts), such as call detail records as well as 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 the Unified CCMP system and ensuring that those changes are updated onto the Unified ICM/Unified CCE and Unified Communications Manager. The Data Import Server component orchestrates the creation, deletion and update of resources to the 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 the 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 the 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 allows for closed-loop management of changes made to dimensions provisioned by the Unified CCMP.

Management Portal: Provisioning Server:

The Provisioning Server is responsible for sending provisioning requests from the Unified CCMP to the Unified CCE. The requests are move, add, change and delete (MACD) operations for the resource types that the Unified CCMP can manage such as creation of new resources, for example a new agent, or new memberships, such as an Agent to Skill Group membership. These updates are applied via the ConAPI interface.

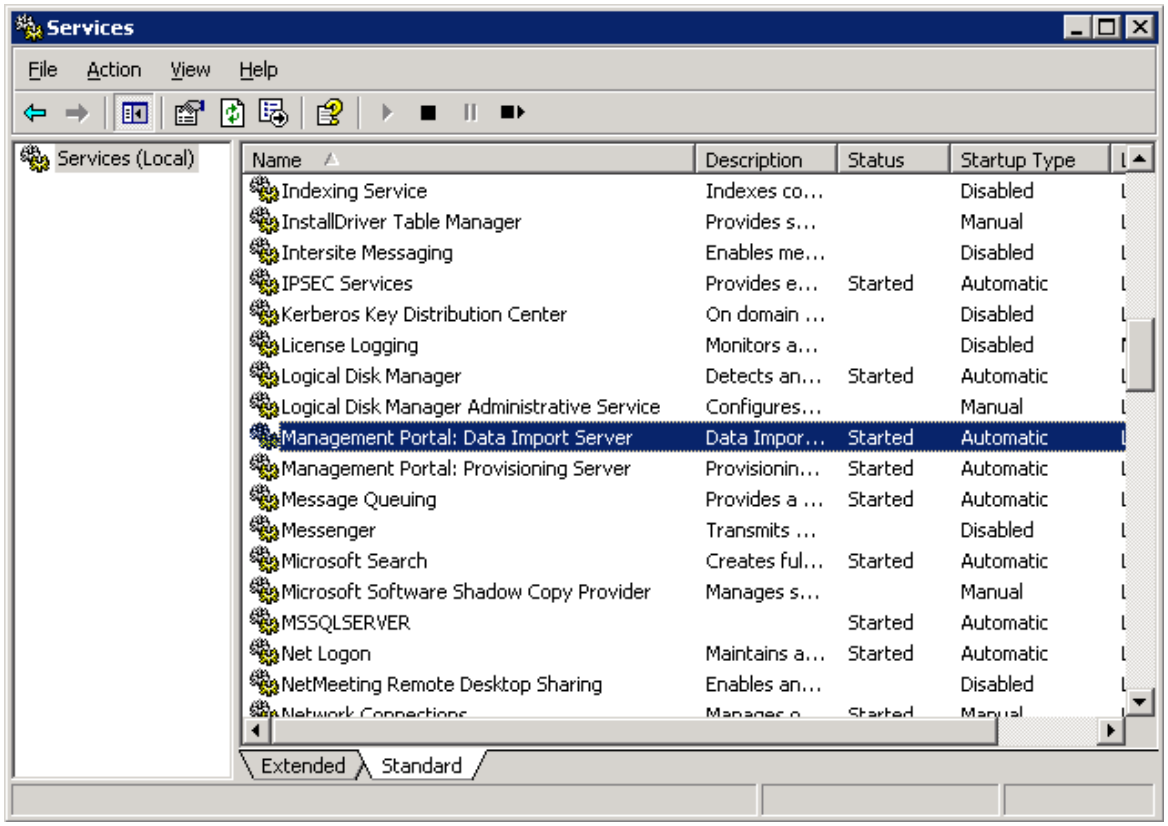


Figure 10: Unified CCMP Services

The 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.

On Windows 2008 R2 systems, a shortcut to **Performance Monitor** is available in the Start Menu > *Cisco Unified CCE Tools* folder. The shortcut launches the 64-bit version of PerfMon so that you can easily monitor the Unified CCE 64-bit process.

2.7 Outbound Option

The 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. The customer uses 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 the 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 the Unified Communications Manager directly using Skinny Call Control Protocol (SCCP) (Communications Manager phone protocol) to perform the dialing. After everything is connected it uses the 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.

Unified CCE Release 8.0(1) offers the Session Initiation Protocol (SIP) Dialer alongside the SCCP Dialer that has been the sole Dialer offered in previous releases of Outbound Option. In an Outbound Option deployment that uses the SIP Dialer, functions such as dialing, call control, and Call Progress Analysis for Outbound campaigns are handled by the Voice Gateway, and not by the Unified CM. This increases the number of Outbound agents that a deployment can service on a PG, and reduces the number of PGs and Dialers customers need to deploy 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.

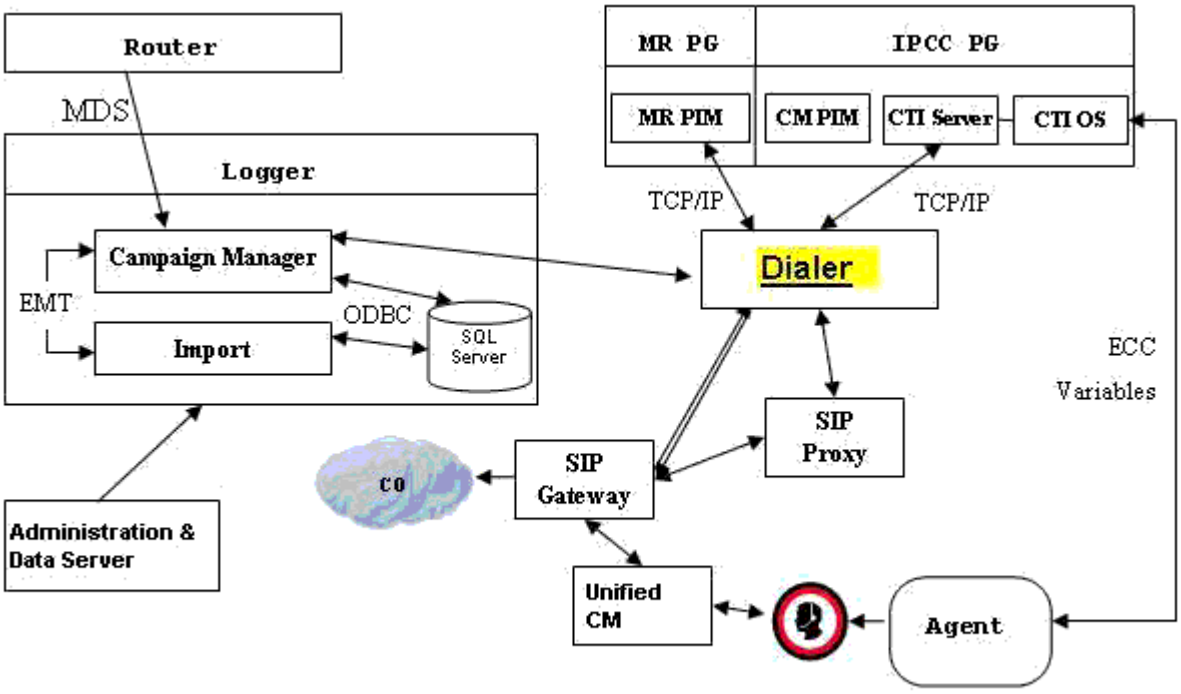


Figure 11: Outbound Option Component Relationships

3 Monitoring SNMP Health

The following section provides an overview of SNMP Health Monitoring.

3.1 SNMP Overview

3.1.1 Faults

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

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

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

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

```
cccaIcmEvent NOTIFICATION-TYPE
   OBJECTS {
      cccaEventComponentId,
      cccaEventState,
      cccaEventMessageId,
      cccaEventOriginatingNode,
      cccaEventOriginatingNodeType,
      cccaEventOriginatingProcessName,
      cccaEventOriginatingSide,
      cccaEventDmpId,
      cccaEventSeverity,
      cccaEventTimestamp,
      cccaEventText
   }
```

A detailed description of each object in the notification type is found in section 4.1.

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

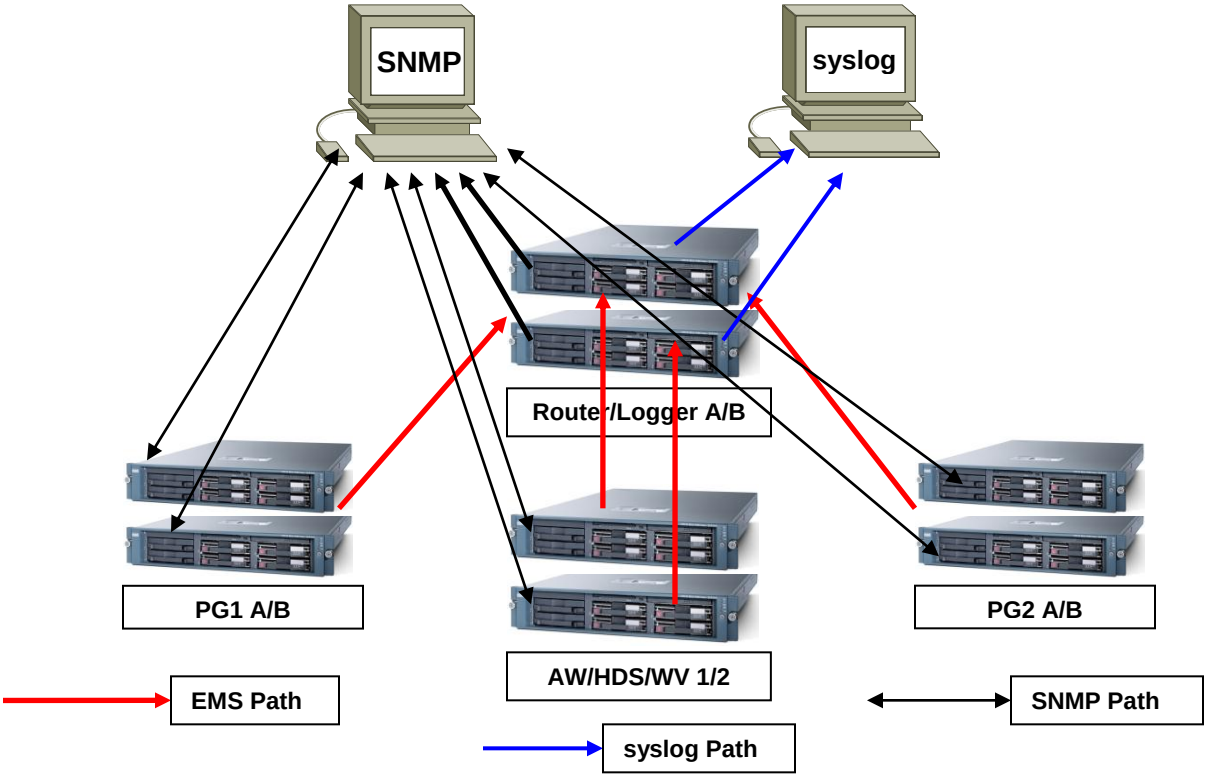


Figure 12: ICM/CCE Event Message Flow

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 the 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.

3.1.2 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 the 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.

3.2 Base-Level SNMP MIB Support

3.2.1 SNMP Master Agent

The 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 herein. 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 (such as the HP/IBM platform MIB subagents noted above) 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/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.

3.2.2 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.

3.2.2.1 Platform MIB Support

A platform MIB/subagent is provided by the hardware vendor – in case of the Cisco Media Convergence Server (MCS) platform, IBM. This subagent provides instrumentation for low-level attributes of the specific hardware:

- IBM-SYSTEM-AGENT-MIB
- IBM-SYSTEM-ASSETID-MIB
- IBM-SYSTEM-HEALTH-MIB

- IBM-SYSTEM-LMSENSOR-MIB
- IBM-SYSTEM-MEMORY-MIB
- IBM-SYSTEM-MIB
- IBM-SYSTEM-NETWORK-MIB
- IBM-SYSTEM-POWER-MIB
- IBM-SYSTEM-PROCESSOR-MIB
- IBM-SYSTEM-RAID-MIB
- IBM-SYSTEM-TRAP-MIB

3.2.2.2 Host Resources MIB Subagent

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

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

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

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

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

cccaComponentElmtName.0.1.5 = router

```
cccaComponentElmtRunID.0.1.5 = 4040
cccaComponentElmtStatus.0.1.5 = active(5)

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

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

3.2.2.3 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.

Installation of the CDP driver and CDP subagent is optional on the Unified ICM/Unified CCE because installation on Cisco MCS servers is not guaranteed (that is to say, Unified ICM is supported on non-MCS hardware).

Note: 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.

3.2.2.4 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.

3.2.2.5 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. For more information, see the sysApplInstallPkgTable.

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.

3.3 CISCO-CONTACT-CENTER-APPS-MIB

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

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

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

3.3.1 CISCO-CONTACT-CENTER-APPS-MIB Overview

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

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

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

3.3.2 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:

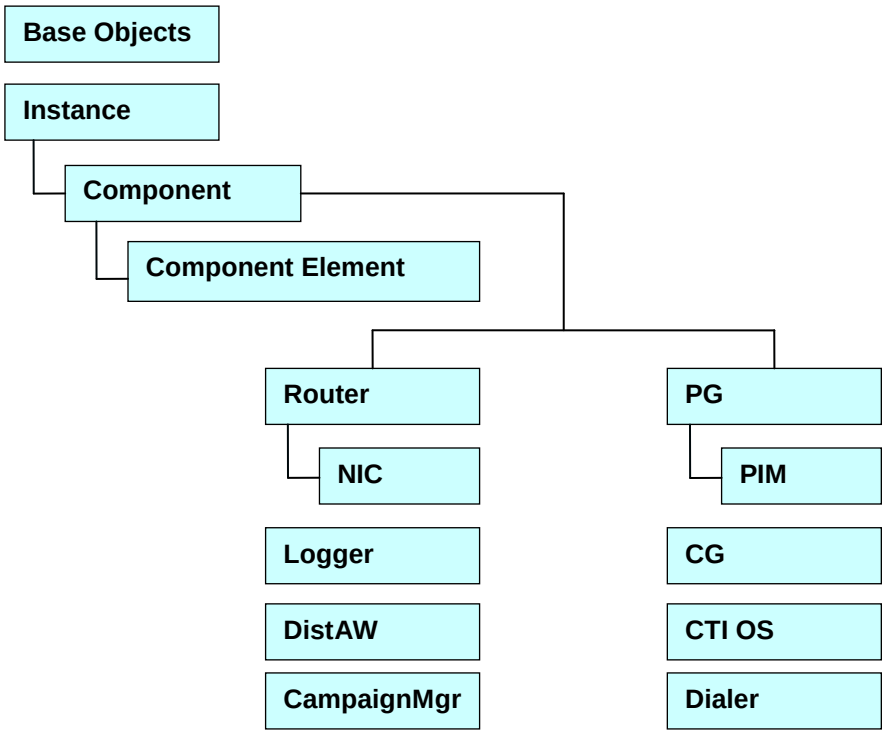


Figure 13: CISCO-CONTACT-CENTER-APPS-MIB Structure

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 the 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:

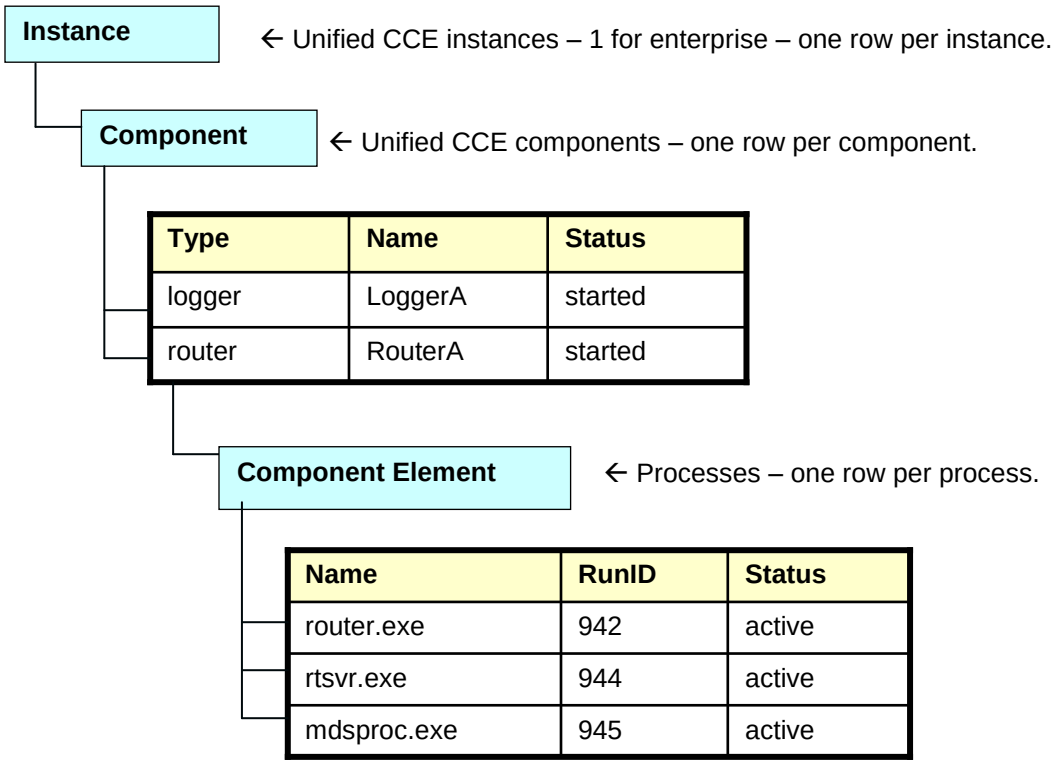


Figure 14: CCCA MIB – Component Inventory Example

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 Figure 16 is an example, only; there can be many more processes listed in the Component Element table.

3.3.3 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.

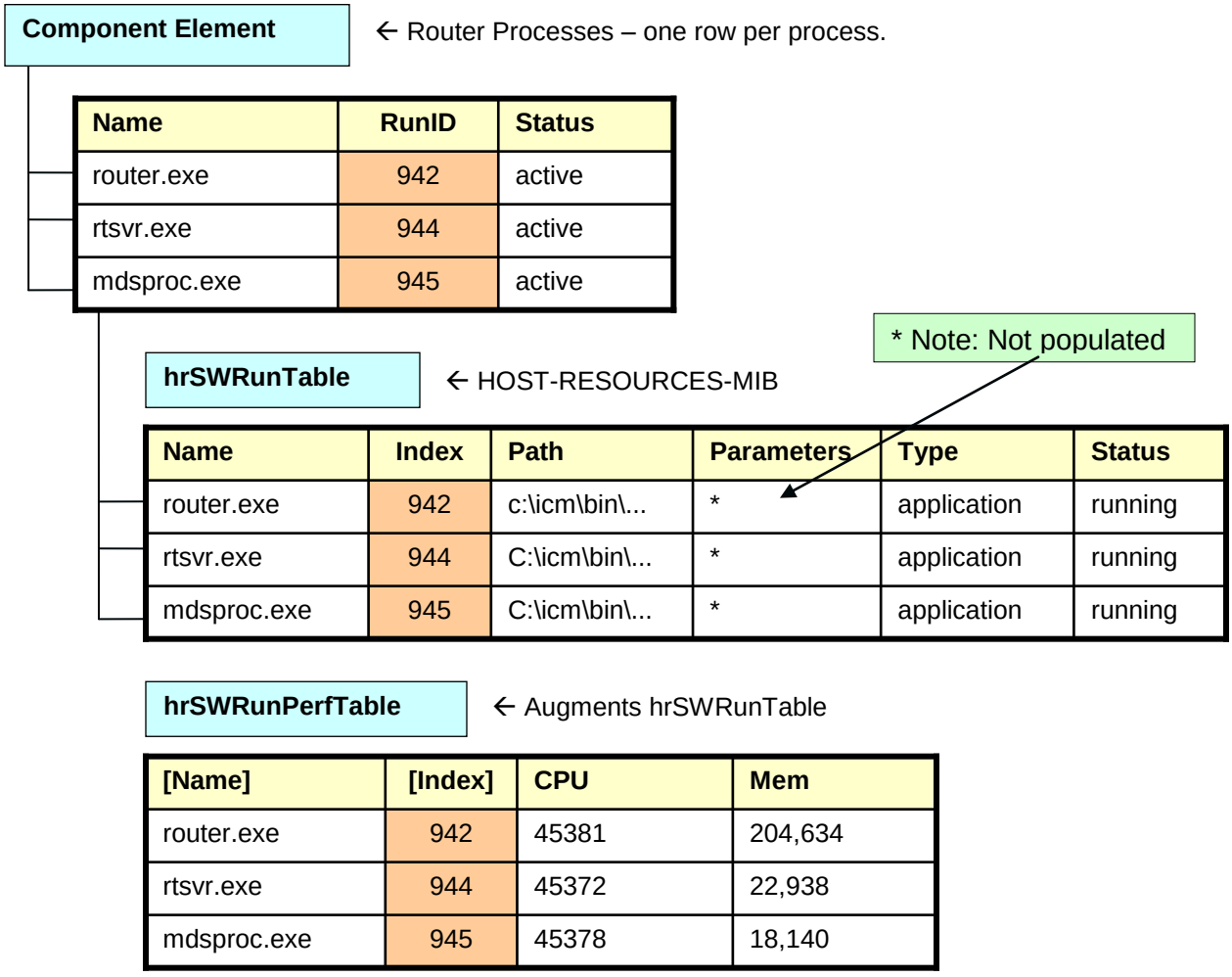


Figure 15: Mapping CCCA MIB Objects to Host MIB Objects

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 the Unified CCE. The application could also poll the remaining rows of the hrSWRunTable/hrSWRunPerfTable for processes that are consuming excessive CPU cycles and/or system memory.

You must note that there is some level of interpretation open to an implementer of a HOST-RESOURCES-MIB subagent. The implementer may decide that some columns of the table

cannot be implemented or simply are not necessary. There are no strict rules. That some objects within these tables do not have values is not necessarily indicative of a failed implementation.

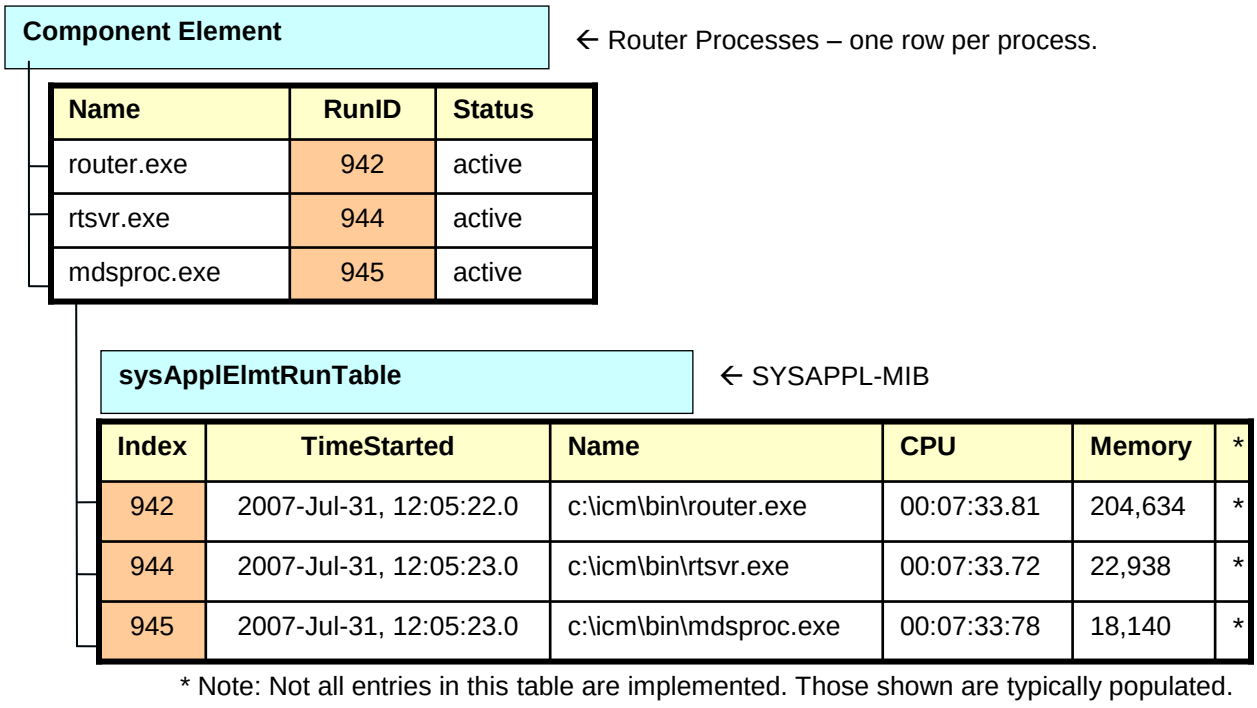


Figure 16: Mapping CCCA MIB to SYSAPPL MIB

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

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. For more information about the notification type object, see section 4.1 for more details about the notification type object.

3.3.4 CISCO-CONTACT-CENTER-APPS-MIB Object Descriptions

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

Table 3-1: CCCA MIB Base Objects

Object Name	Description
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	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

Object Name	Description
	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.

Table 3-2: CCCA MIB Instance Table Objects

Object Name	Description
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.

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.

Table 3-3: CCCA MIB Component Table Objects

Object Name	Description
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

Object Name	Description
	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.

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.

Table 3-4: CCCA MIB Component Element Table Objects

Object Name	Description
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 sysApplElmtRunIndex value of sysApplElmtRunTable 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

Object Name	Description
	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.

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 sysApplElmtRunTable 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.

Table 3-5: CCCA MIB Router Table Objects

Object Name	Description
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

Object Name	Description
	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.
cccaRouterPublicNonHighAddr	The Router public non-high address object holds the address

Object Name	Description
	of the local interface of this Router functional component to the public network that is used for best effort priority messages. The public network interface is exposed outside the realm of the Unified ICM or Unified CC application and is used for the transfer of data between this Router and other functional components of the deployment. This interface is used for normal-priority messages.
cccaRouterPrivateHighAddr	The Router private high address object holds the address of the local high-priority interface of this Router functional component to the private network. The private network interface is used exclusively by the Unified ICM or Unified Contact Center application for the transfer of synchronization data between duplexed pairs and for the transfer of application data from the Router to the Logger. This interface is reserved for high-priority messages and as much as 90% of the available network bandwidth is allocated to this interface.
cccaRouterPrivateNonHighAddr	The Router private non-high address object holds the address of the local interface of this Router functional component to the private network that is used for best effort priority messages. The private network is used exclusively by the Unified ICM or Unified Contact Center application for the transfer of synchronization data between duplexed pairs and for the transfer of application data from the Router to the Logger. This interface is used for normal-priority messages.

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.

Table 3-6: CCCA MIB NIC Table Objects

Object Name	Description
cccaNicIndex	A value that uniquely identifies an entry in the network interface controller table. The value of this object is arbitrarily assigned by the SNMP subagent.
cccaNicType	Indicates to which telephony network this NIC functional component provides an interface.
cccaNicStatus	The last known status of the enterprise contact center application network interface controller functional component.

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.

Table 3-7: CCCA MIB Logger Table Objects

Object Name	Description
cccaLoggerSide	Which of the duplex pair this entry represents, of an enterprise contact center application fault tolerant Logger functional component. The Logger side value is either 'A' or 'B'. For simplex configurations, the Logger side value defaults to 'A'.
cccaLoggerType	Which type of enterprise contact center application Logger, is installed on this server. The Logger type varies based on the configuration of the contact center solution.
cccaLoggerRouterSideAName	The hostname of the side 'A' Router that this enterprise contact center application Logger functional component is associated. The Logger component must be connected to a Router that is part of the same instance.
cccaLoggerRouterSideBName	The hostname of the side 'B' Router that this enterprise contact center application Logger functional component is associated. The Logger component must be connected to a Router that is part of the same instance.
cccaLoggerDuplexPairName	The hostname of the duplex pair (for example, the other side) server of an enterprise contact center application fault tolerant Logger component. If this component is not part of a duplex pair (for example, simplex), the object value is the null string. The Logger connects to its duplex pair via a private' interface – a closed subnet that guarantees a quality of service level that does not impact the performance of the contact center application. This private subnet is not accessible by the management station.
cccaLoggerHDSReplication	Indicates whether the Logger component replicates data to a Administration Server, Real-time and Historical Data Server, and Detail Data Server. If true, the Logger feeds historical data at regular intervals to the HDS for long-term storage. In this configuration, administrator reports are generated by accessing data from the HDS rather than the Logger in order to remove the performance impact of reporting on the Logger.
cccaLoggerAvgDBWriteTime	The Logger average database write time expresses the average amount of time, in 100 nanosecond units, required to write data to a table in the central controller database. This

Object Name	Description
	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.

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.

Table 3-8: CCCA MIB Administration Server and Real-time Data Server Table Objects

Object Name	Description
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

Object Name	Description
	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	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.
cccaDistAwWebViewServer Name	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

Object Name	Description
	historical data that is requested when generating reports..
cccaDistAwWebReskillingURL	The administration and data server web re-skilling URL object holds the URL for the contact center application web re-skilling tool. The web re-skilling tool allows contact center administrators and supervisors to re-skill agents (reassign contact center agents to different skill groups allowing them to take calls of a different topic).

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.

Table 3-9: CCCA MIB Peripheral Gateway Table Objects

Object Name	Description
cccaPgNumber	A user-defined numeric identifier for this enterprise contact center application peripheral gateway. The value is limited by the contact center application to a value between 1 and 80; 80 is the maximum number of peripheral gateways supported by the architecture.
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

Object Name	Description
	Router.
cccaPgDuplexPairName	The hostname of the duplex pair (for example, the other side) server of an enterprise contact center application fault tolerant peripheral gateway component. If this component is not part of a duplex pair (for example, simplex), the object value is the null string.
cccaPgPimCount	The number of peripheral interface managers configured and enabled for this enterprise contact center application peripheral gateway functional component. This value is limited to 32−this is the maximum number of PIMs supported on a single peripheral gateway.
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.

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.

Table 3-10: CCCA MIB Peripheral Interface Manager Table Objects

Object Name	Description
cccaPimNumber	The numeric identifier for this enterprise contact center application PIM. This object value is a user-defined numeric value and is limited to a maximum of 32 because this is the maximum number of PIMs supported on a single peripheral gateway.
cccaPimPeripheralName	The user-defined textual name of the enterprise contact center application PIM. This name uniquely identifies the PIM.

cccaPimPeripheralType	The type of the enterprise contact center application PIM, for example, the brand name and model of the ACD, private branch exchange (PBX), or VRU.
cccaPimStatus	The last known status of the enterprise contact center application peripheral interface manager functional component.
cccaPimPeripheralHostName	The hostname or IP address of the peripheral (the PBX, ACD, or VRU) to which the enterprise contact center application PIM is connected. If there are multiple interfaces to the peripheral, each hostname or IP address is separated by a comma.

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.

Table 3-11: CCCA MIB CTI Gateway Table Objects

Object Name	Description
cccaCgNumber	A numeric identifier for this enterprise contact center application CTI Gateway. This is a user-defined numeric value and may not be identical to the table index. The value is limited by the contact center application to a value between 1 and 80 as this is the maximum number of CTI gateways supported by the architecture.
cccaCgSide	Which of the duplex pair this entry represents of an enterprise contact center application fault tolerant CTI gateway functional component. The CG side value is either 'A' or 'B'. For simplex configurations, the CG side value defaults to 'A'.
cccaCgPgSideAName	The hostname of the side ‘A’ PG that this enterprise contact center application CTI gateway (CG) functional component is associated. The CG component must be connected to a PG that is part of the same instance. If the side ‘B’ PG is the active PG and a failure occurs, the side ‘A’ PG then immediately assumes the role. In this case, the CG loses its connection to the side ‘B’ PG and thus use this object value to connect to the side ‘A’ PG.
cccaCgPgSideBName	The hostname of the side ‘B’ peripheral gateway (PG) that this enterprise contact center application CTI gateway (CG) functional component is associated. The CG component must be connected to a PG that is part of the same instance. If the

Object Name	Description
	side 'A' PG is the active PG and a failure occurs, the side 'B' PG then immediately assumes the role. In this case, the CG loses its connection to the side 'A' PG and thus use this object value to connect to the side 'B' PG.
cccaCgDuplexPairName	The hostname of the duplex pair (for example, the other side) server of an enterprise contact center application fault tolerant CTI gateway component. If this component is not part of a duplex pair (for example, simplex), the object value is the null string.
cccaCgOpenSessions	The CG open sessions object indicates the number of sessions (connections) that were established between the CTI Gateway and CTI clients. These are active sessions that are functioning normally.
cccaCgOtherSessions	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.
cccaCgID	The CG number is a unique numeric identifier for this enterprise contact center application CTI gateway. The identifier is assigned by the contact center application.

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.

Table 3-12: CCCA MIB CTI OS Table Objects

Object Name	Description
cccaCtiOsServerName	The user-defined textual name assigned to this enterprise contact center application CTI OS component to uniquely identify it.
cccaCtiOsPeripheralName	The unique identifier for the peripheral that the enterprise contact center application CTI OS component is associated. This association links the CTI desktop clients with a particular peripheral PBX.
cccaCtiOsPeripheralType	The peripheral type that the enterprise contact center application CTI OS is associated. This also then identifies the peripheral PBX type that the CTI desktop clients are

Object Name	Description
	associated.
cccaCtiOsCgSideAName	The hostname of the side 'A' CTI gateway (CG) that this enterprise contact center application CTI object server (CTI OS) functional component is associated. The CTI OS component must be connected to a CG that is part of the same instance. If the side 'B' CG is the active CG and a failure occurs, the side 'A' CG then immediately assumes the role. In this case, CTI OS loses its connection to the side 'B' CG and thus use this object value to connect to the side 'A' CG.
cccaCtiOsCgSideBName	The hostname of the side 'B' CTI gateway (CG) that this enterprise contact center application CTI OS functional component is associated. The CTI OS component must be connected to a CG that is part of the same instance. If the side 'A' CG is the active CG and a failure occurs, the side 'B' CG then immediately assumes the role. In this case, CTI OS loses its connection to the side 'A' CG and thus use this object value to connect to the side 'B' CG.
cccaCtiOsPeerName	The hostname of the peer server of an enterprise contact center application CTI object server functional component. If this component does not have a peer, the object value is the null string. Note that the CTI OS component implements fault tolerance slightly differently than other components of the contact center solution. CTI OS maintains two active peer object servers to serve client desktop CTI applications. If a failure occurs on one of the two servers, its clients connect to the peer server.
cccaCtiOsActiveClients	The active clients object holds the number of CTI OS active client mode desktop connections. This value indicates the total number of desktops connected to the CTI OS server. The number of desktops connected to the A and B side of CTI OS determine the total desktops connected through this instance of CTI OS server.
cccaCtiOsActiveMonitors	The active monitors object holds the number of CTI OS active monitor mode desktop connections. CTI OS only supports two monitor mode connections per each CTI OS server. This value indicates how many monitor mode connections are in use. After there are two in use further monitor mode connection attempts are rejected.
cccaCtiOsCallsInProgress	The calls in progress object indicate the total number of active calls being tracked by CTI OS. This value shows how many calls are currently being handled by CTI OS. This value should go up and down based on the call arrival rate and the agent call completion rate.
cccaCtiOsCallsFailed	The calls failed object holds the total number of calls that failed via a failure event being reported to CTI OS. If this count begins to rise, the log file should be captured to gather

Object Name	Description
	more specific information about the failure events.

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.

Table 3-13: CCCA MIB Outbound Option Campaign Manager Table Objects

Object Name	Description
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 start paying attention when this 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.

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.

Table 3-14: CCCA MIB Outbound Option Dialer Table Objects

Object Name	Description
cccaDialerCampaignMgrName	The Dialer campaign manager name object holds the hostname or IP address of the Outbound Option Campaign Manager to which this Dialer is associated. The Dialer connects to the campaign manager to exchange data related to an Outbound Dialing campaign.
cccaDialerCampaignMgrStatus	The Dialer campaign manager status indicates the current connection status between this Dialer and the Outbound Option Campaign Manager component, which is coresident with the Logger (side A).
cccaDialerCtiServerAName	The Dialer CTI server A name object holds the hostname or IP address of the contact center application CTI Server side A functional component, which this Dialer depends. The Dialer connects to the CTI Server to monitor skill group statistics (to choose an agent) and executes call control after an available agent is selected.
cccaDialerCtiServerBName	The Dialer CTI server B name object holds the hostname or IP address of the contact center application CTI Server side B functional component, which this Dialer depends. The Dialer connects to the CTI Server to monitor skill group statistics (to choose an agent) and executes call control after an available agent is selected.
cccaDialerCtiServerStatus	The Dialer CTI server status indicates the current connection status between this Dialer and the active CTI server component.

Object Name	Description
cccaDialerMediaRouterStatus	The Dialer media Router status indicates the current connection status between this Dialer and the Media Routing (MR) Peripheral Interface Manager (PIM) component. The Dialer uses the MR PIM interface to reserve an available agent as a recipient for a dialed customer call.
cccaDialerQueueDepth	The Dialer is a multithreaded process that communicates between threads using inter-thread messaging. The queue depth object indicates how many messages are currently queued for the main dispatch thread. When this object is used in combination with the average queue time object, message processing performance can be gauged. 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

Object Name	Description
	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.

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.

3.4 Configuring the SNMP Agents

3.4.1 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.

3.4.2 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.

3.4.3 Adding the Cisco SNMP Agent Management Snap-in

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:

1. From the Start menu select **Run**.
2. In the Start box type in **mmc** and press <Enter>.
3. From the Console, select **File > Add/Remove Snap-in**

   A new window appears.
4. From the **Standalone** tab, verify **Console Root** is selected in the **Snap-ins added to:** field and click **Add**.
5. In the Add Snap-in window scroll down and select **Cisco SNMP Agent Management**.
6. In the Add Snap-in window click **Add**.
7. In the Add Snap-in window click **Close**.
8. Click **OK** in the **Add/Remove Snap-in** window.

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

3.4.4 Saving the 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. To do so, select the **Console > Save As** menu; a **Save As** dialog appears.

Select a memorable file name such as **Cisco SNMP Agent Management.msc** (retain the .msc file extension) and 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.

The system administrator must configure the following to grant access to the agents and enable the receipt of SNMP notifications:

SNMP v1/v2c Community Name

OR

SNMP v3 User Names

AND

SNMP Trap Destination(s)

If using SNMP Version 1 or Version 2c, you must configure at least one community on each Unified ICM/Unified CCE server to be managed, OR

If using SNMP Version 3, you must configure at least one user name on each Unified ICM/Unified CCE server to be managed.

To receive SNMP notifications at a network management station, you must configure an SNMP trap destination on each Unified ICM/Unified CCE server. You can also optionally add a syslog destination on a Unified ICM/Unified CCE Logger server. Unified ICM/Unified CCE notifications are only sent from the Unified ICM/Unified CCE Logger; however, to receive standard SNMP notifications (for example, Link Up or Link Down notifications), you must configure a trap destination on all Unified ICM/Unified CCE servers.

Note: Some diagnostic tools may use SNMP locally to gather information about the system using one of the community strings configured for Windows SNMP. These community strings are not added to the Contact Center SNMP configuration, which causes SNMP requests from these diagnostic tools to fail. You can add all communities configured for Windows SNMP to the Contact Center SNMP configuration. It is not necessary for the Windows SNMP service to be started or enabled. You can find the Windows SNMP communities in the Security tab by selecting properties for the Windows SNMP service from the list of Windows services.

3.4.5 Configuring 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:

1. Expand **Cisco SNMP Agent Management** in the left pane of the MMC snap-in.
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.
3. Right-click the white space in the right pane and choose **Properties.**

   A dialog box appears.
4. Click **Add new Community**.
5. In the dialog box, under **Community Information**, provide a community name.
6. Select the **SNMP Version** by selecting the radio box for SNMP v1 or SNMP V2c.
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.
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.

   Changes become effective when you click **OK**.

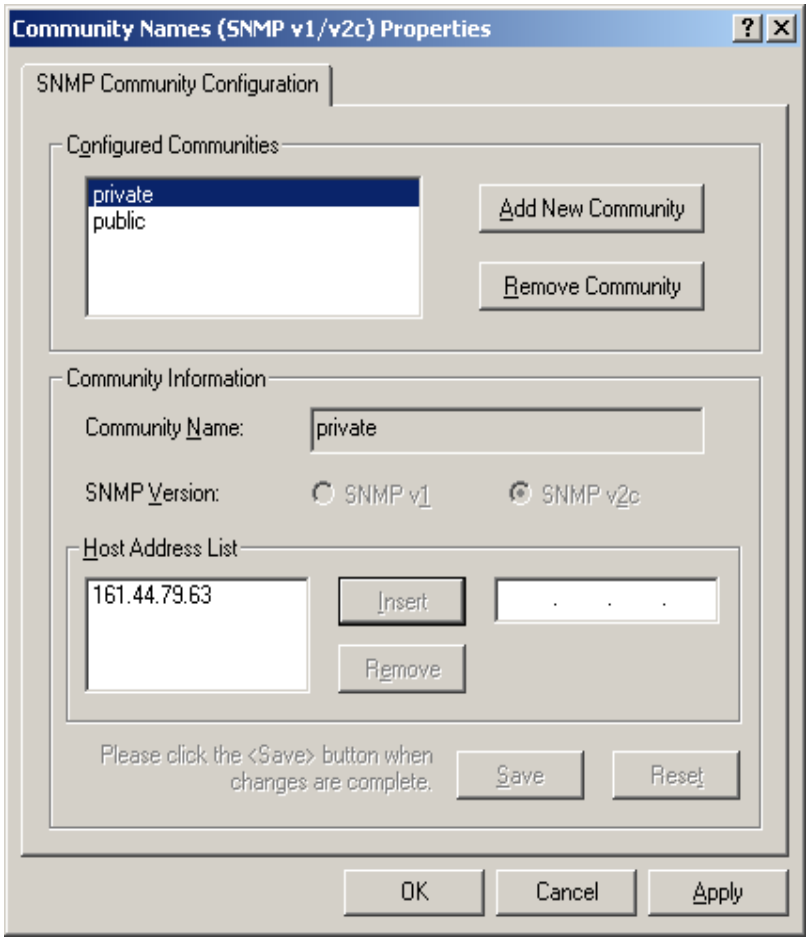


Figure 17: SNMP Community Name Configuration Dialog

3.4.6 Configuring 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.

To configure a User Name for SNMP v3:

1. Expand **Cisco SNMP Agent Management** in the left pane of the MMC snap-in.
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.
3. Right-click the white space in the right pane and choose **Properties.**

   A dialog box appears.
4. Click **Add User**.
5. In the **User Configuration** text box enter a user name.
6. If you wish to use SNMP v3 authentication, check **Required?** under Authentication and choose an authentication protocol; then 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.

7. If you wish to use SNMP v3 privacy, check **Required?** under Privacy and choose an encryption type; then 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.

8. Optionally, 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.
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 Name by highlighting the name in the Configured Users section and clicking Remove User.

   Changes become effective when you click **OK**.

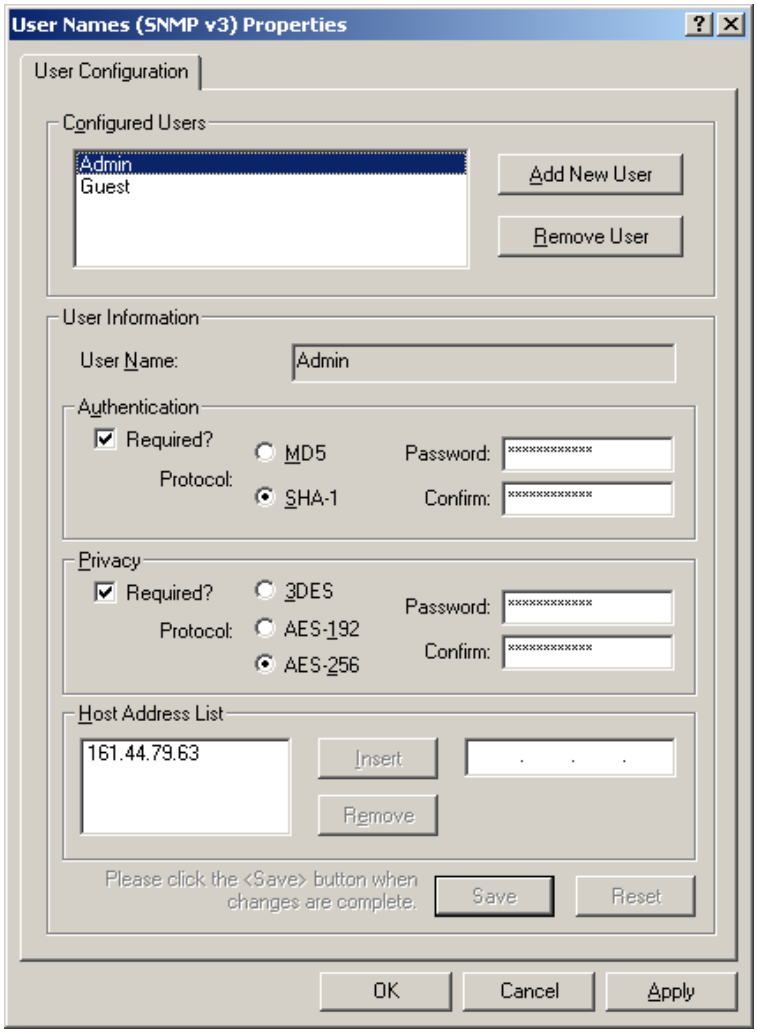


Figure 18: SNMP User Name Configuration Dialog Box

3.4.7 Configuring General Information Properties

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

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

   A dialog box appears.
3. You can change the following properties in the **SNMP System Information** section of the General Information Properties dialog box.

Table 3-15: SNMP General Information Properties

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

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

You can change the Windows Execution Priority of the Cisco SNMP agents in the **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.

You can also further 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.

3.4.8 Definition of Agent Performance Settings

Definition	Description
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.

You can change the amount of information written to the SNMP logs by choosing Verbose (most information), Normal (Default), or Terse (least information). Change this value only under direction from Cisco Technical Assistance (TAC).

Note: You can retrieve logs using the Analysis Manager.

Click **OK** to save any changes you have made.

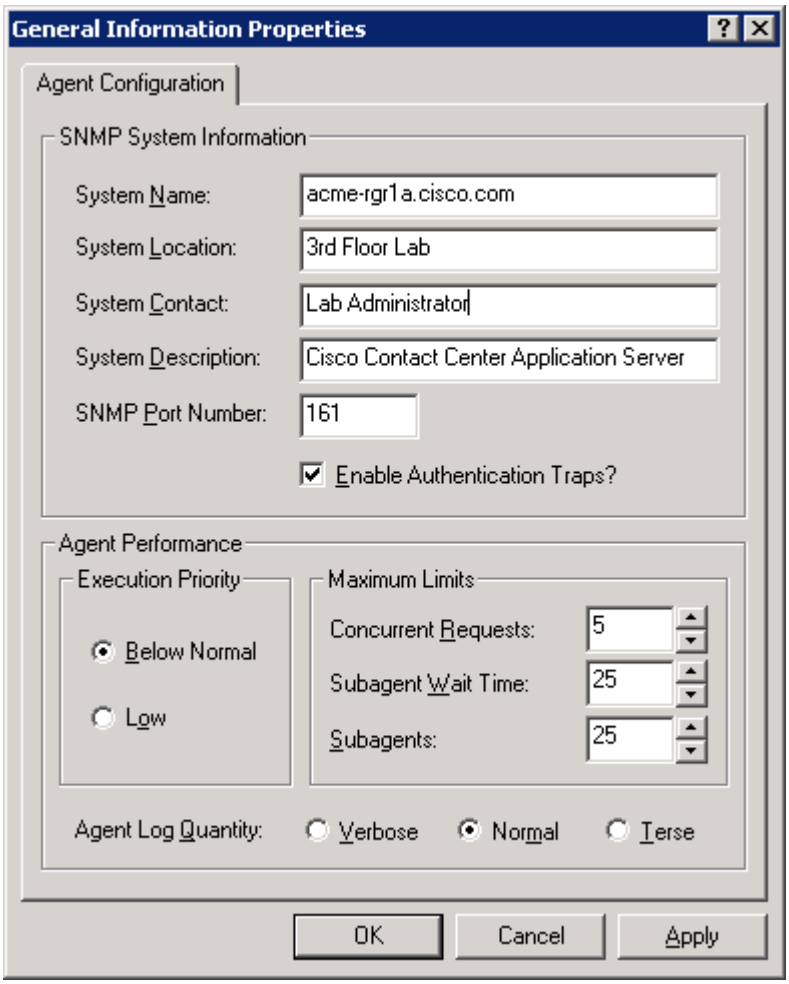


Figure 19: SNMP General Information Configuration Dialog Box

3.4.9 Configuring 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. To configure the trap destinations:

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

   A dialog box appears.
4. Click **Add Trap Entity.**
5. Under **Trap Entity Information** select the SNMP version radio box for the version of SNMP used by your NMS.
6. Provide a name for the trap entity in the **Trap Entity Name** field.
7. Select the SNMP Version Number.
8. Select the User Name/Community Name that you want to associate with this trap. This list is auto-populated with existing users/community names that have been configured.
9. Enter one or more IP addresses in the IP Address entry field (containing "dots") and click **Insert** to define the destinations for the traps.
10. Click **Save** to save the new 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**.

Changes become effective when you click **OK**.

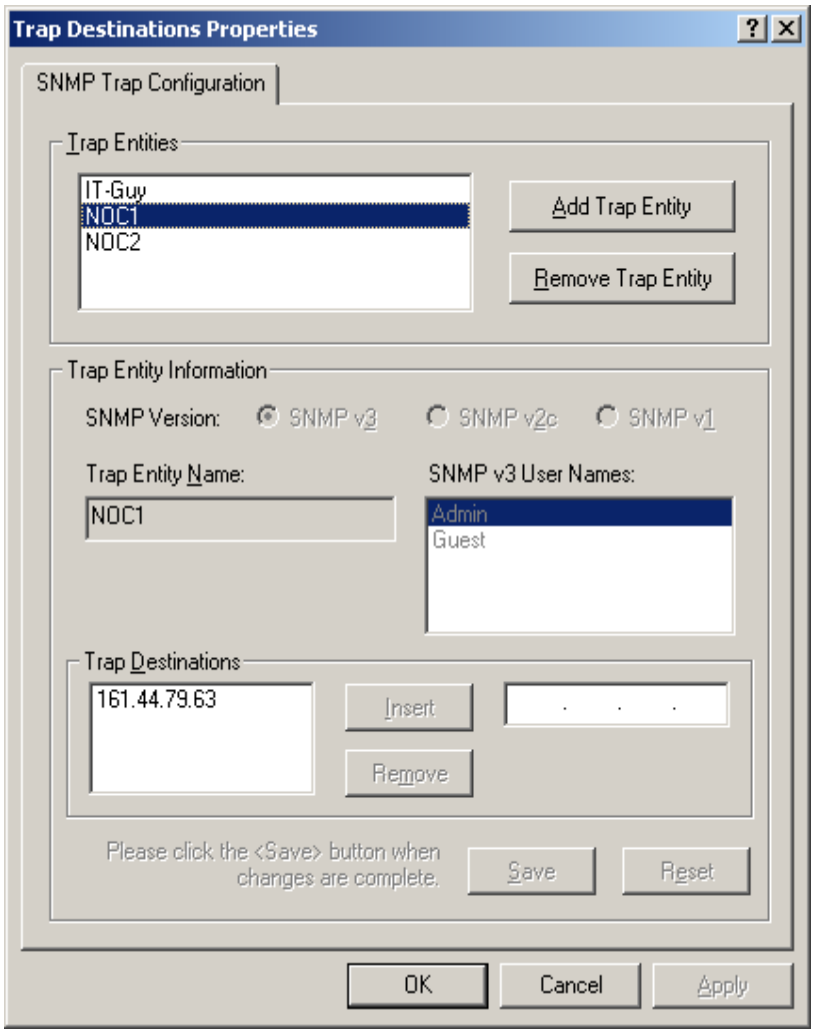


Figure 20: SNMP Trap Destination Configuration Dialog Box

4 Understanding Unified ICM/Unified CCE SNMP Notifications

Most Unified ICM/Unified CCE SNMP notifications are "stateful" events; each event correlates to a managed object. An object is defined as having dual state or single state.

4.1 Unified ICM/Unified CCE Notification Type

4.1.1 cccaIcmEvent

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

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

Table 4-1: Unified ICM/Unified CCE Notification Type Objects

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

Object Name	Description
	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.
cccaEventOriginatingNodeType	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.
cccaEventOriginatingProcessName	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.
cccaEventOriginatingSide	The enterprise contact center application functional component fault tolerant side (either 'A' or 'B') that generated this notification.
cccaEventDmpId	The Device Management Protocol (DMP) is a session layer protocol used for network communication between enterprise contact center application functional components. The DMP

Object Name	Description
	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.
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.

4.2 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.

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

snmpTrapOID.0 = cccaIcmEvent
cccaEventComponentId = 4_1_CC-RGR1A_ICM\acme\RouterA
cccaEventState = raise(4
cccaEventMessageId = 2701295877
cccaEventOriginatingNode = CC-RGR1A\acme
cccaEventOriginatingNodeType = router(1)

cccaEventOriginatingProcessName = nm
cccaEventOriginatingSide = sideA(1)
cccaEventDmpId = 0
cccaEventSeverity = warning(2)
cccaEventTimestamp = 2006-03-31,14:19:42.0
cccaEventText = The operator/administrator has shutdown the ICM software on ICM\acme\RouterA

snmpTrapOID.0 = cccaIcmEvent
cccaEventComponentId = 4_1_CC-RGR1A_ICM\acme\RouterA
cccaEventState = clear(0)
cccaEventMessageId = 1627554051
cccaEventOriginatingNode = CC-RGR1A\acme
cccaEventOriginatingNodeType = router(1
cccaEventOriginatingProcessName = nm
cccaEventOriginatingSide = sideA(1)
cccaEventDmpId = 0
cccaEventSeverity = informational(1)
cccaEventTimestamp = 2006-03-31,13:54:12.0
cccaEventText = ICM\acme\RouterA Node Manager started. Last shutdown was by operator request.

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

Table 4-2: Example "Raise" Notification

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

Table 4-3: Example "Clear" Notification

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

4.3 Correlating Dual State Notifications

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

- **"Raise" Event:**

  cccaEventComponentId: **"4_1_acme-rgr_ICM\acme\RouterA"**
  Event Class: **CLASS_NM_INITIALIZING**
  cccaEventState: **raise(4)**
  cccaEventMessageId: **2701295877**
  cccaEventSeverity: **warning(2)**
  cccaEventText: The operator/administrator has shutdown the ICM software on ICM\acme\RouterA.

- **"Clear" Event**

  cccaEventComponentId: **"4_1_acme-rgr_ICM\acme\RouterA"**
  Event Class: **CLASS_NM_INITIALIZING**
  cccaEventState: **clear(0)**
  cccaEventMessageId: **1627554051**
  cccaEventSeverity: **informational(1)**
  cccaEventText: ICM\acme\RouterA Node Manager started. Last shutdown was by operator request.

- ✓ Upon receipt of "Raise" event, categorize by severity
- ✓ Upon receipt of "Clear" event, match to "Raise" using 'cccaEventComponentId'

In the above example notifications, a simple string comparison of "" can suffice in matching the clear to the raise. cccaEventComponentId has the event class built into this value and the rest of

the string was crafted to be sufficiently unique to ensure that the appropriate raises are cleared by the clear notification. (Remember: Multiple raise notifications can be cleared by a single clear notification.)

Sample logic:

```
If (cccaEventState == "clear")
    set ID = cccaEventComponentId;
    for (all "raise" events where cccaEventComponentId == ID)
        Acknowledge();
```

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

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

4.4 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 4-4: Example "Single-State Raise" Notification

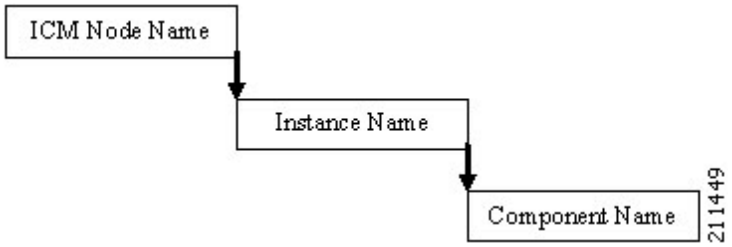
Field	Value / Description
NOTIFICATION	105023C
cccaEventMessageId	3775201852 (0xE105023C)
DESCRIPTION	The Router has detected that it is no longer synchronized with its partner. One result of this is that the Router might be routing some calls incorrectly.
cccaEventState	**Single-state Raise**
SUBSTITUTION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

Field	Value / Description
cccaEventComponentId	{ cccaEventOriginatingNode cccaEventOriginatingProcessName cccaEventOriginatingSide }
CorrelationId	{ CLASS_RTR_SYNC_CHECK cccaEventOriginatingNode cccaEventOriginatingProcessName cccaEventOriginatingSide }

4.5 Organizing SNMP Notifications

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

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



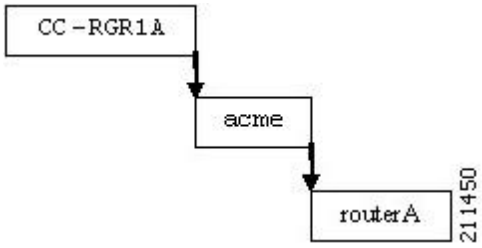
where:

Unified ICM/CCE Node Name = left side of cccaEventOriginatingNode

Instance Name = right side of cccaEventOriginatingNode

Component Name = cccaEventOriginatingNodeType + cccaEventOriginatingSide letter

For example:



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

4.6 CSFS Heartbeat Notification

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

Table 4-5: CSFS Heartbeat Notification

Field	Value / Description
NOTIFICATION	12A0003
cccaEventMessageId	1630142467 (0x612A0003)
DESCRIPTION	Periodic message to indicate MDS is in service and that the event stream is active.
cccaEventState	
SUBSTITUTION STRING	HeartBeat Event for %1
ACTION	No action is required.
cccaEventComponentId	{ cccaEventOriginatingNode %1 }
CorrelationId	n/a

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

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

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

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

5 The syslog Messaging Interface

All versions (since Release 4.6(2)) of Unified ICM/Unified CCE have provided a syslog (The BSD syslog Protocol, RFC-3164) event feed; this feed was originally designed for the CiscoWorks family of network management products. As a result, the Logger process that provides the syslog feed is named CW2KFeed (CiscoWorks 2000 Feed); however, it is an RFC-3164 compliance event feed.

The syslog feed provides a more verbose set of notifications than the SNMP notifications – there are many more events sent via syslog than SNMP and the content matches that which is stored in the Unified ICM/Unified CCE database and the Windows Event Log.

You configure the syslog feed using the Microsoft Management Console snap-in – the same MMC snap-in you used to configure the SNMP agents. For more information about configuring the syslog feed, see the following.

The syslog event feed changed with Release 7.2(1) of Unified ICM/Unified CCE to format all events in Cisco Log message format. The Cisco Log message format provides the following key benefits:

- Precisely documented message format for wide interoperability
- Compatible with IOS message format
- Precise message source identification with host, IP address, application, process, and so on
- Message ordering with sequence numbers and timestamp with millisecond precision
- Support for tagging of messages for correlation or external filtering
- Support for internationalization of host, tags, and message text

5.1 The Cisco Log Message Format

The Cisco Log message format is:

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

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

<134>25: host-w3k: Feb 13 2007 18:23:21.408 +0000: %ICM_Router_CallRouter-6-10500FF: [comp=Router-A][pname=rtr][iid=ipcc1][mid=10500FF][sev=info]: Side A rtr process is OK.

The following table describes the Cisco Log message fields:

Table 5-1: Cisco Log Message Fields

Field	Description
PRI	Encodes syslog message severity and syslog facility. Messages are generally sent to a single syslog facility (that is, RFC-3164 facilities local0 through local7). For more information, see RFC-3164.
SEQNUM	Number used to order messages in the time sequence order when multiple messages occur with the same time stamp by the same process. Sequence number begins at zero for the first message fired by a process since the last startup.
HOST	Fully qualified domain name (FQDN), hostname, or IP address of the originating system.
MONTH	Current month represented in MMM format (for example, “Jan” for January)

Field	Description
DAY	Current day represented in DD format. Range is 01 to 31.
YEAR	Current year represented in YYYY format.
HOUR	Hour of the timestamp as two digits in 24-hour format; range is 00 to 23.
MINUTE	Minute of the timestamp as two digits; range is 00 to 59.
SECOND	Second of the timestamp as two digits; range is 00 to 59.
MILLISECONDS	Milliseconds of the timestamp as three digits; range is 000 to 999.
TIMEZONE	Abbreviated time zone offset, set to +/-#### (+/- HHMM from GMT).
APPNAME	Name of the application that generated the event. APPNAME field values are: PRODUCT_COMPONENT_SUBCOMPONENT PRODUCT – such as ICM COMPONENT – such as Router SUBCOMPONENT – such as CallRouter
SEVERITY	Supported severity values are: 3 (Error) 4 (Warning) 6 (Informational) 7 (Debug)
MSGID	Hexadecimal message id that uniquely identifies the message, such as 10500FF.
TAGS	(Optional) Supported tags are: [comp=%s] - component name including side, such as Router-A [pname=%s] - process name, such as rtr [iid=%s] - instance name, such as ipcc1 [mid=%d] - message id, such as 10500FF [sev=%s] – severity, such as info
MESSAGE	A descriptive message about the event.

5.2 Configuring 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.

To configure syslog destinations:

1. Expand **Cisco SNMP Agent Management** in the left pane of the MMC snap-in.
2. Highlight **Syslog Destinations** in the left pane under Cisco SNMP Agent Management. ICM Instance Name, Feed Enabled, Collector Address, Port, and Ping Disabled columns appear in the right pane.
3. Right-click the white space in the right pane and choose **Properties**.

   A dialog box appears.
4. Select a Unified ICM/Unified CCE Instance from the list box.
5. Check the **Enable Feed?** check box.
6. Enter an IP Address or Host Name in the **Collector Address** field.

7. Optionally, enter the collector port number on which the syslog collector is listening in the **Collector Port** field. The default port is 514.
8. Optionally, check the **Disable Ping Tests?** check box.
9. Click **Save**

Changes become effective when you click **OK**.

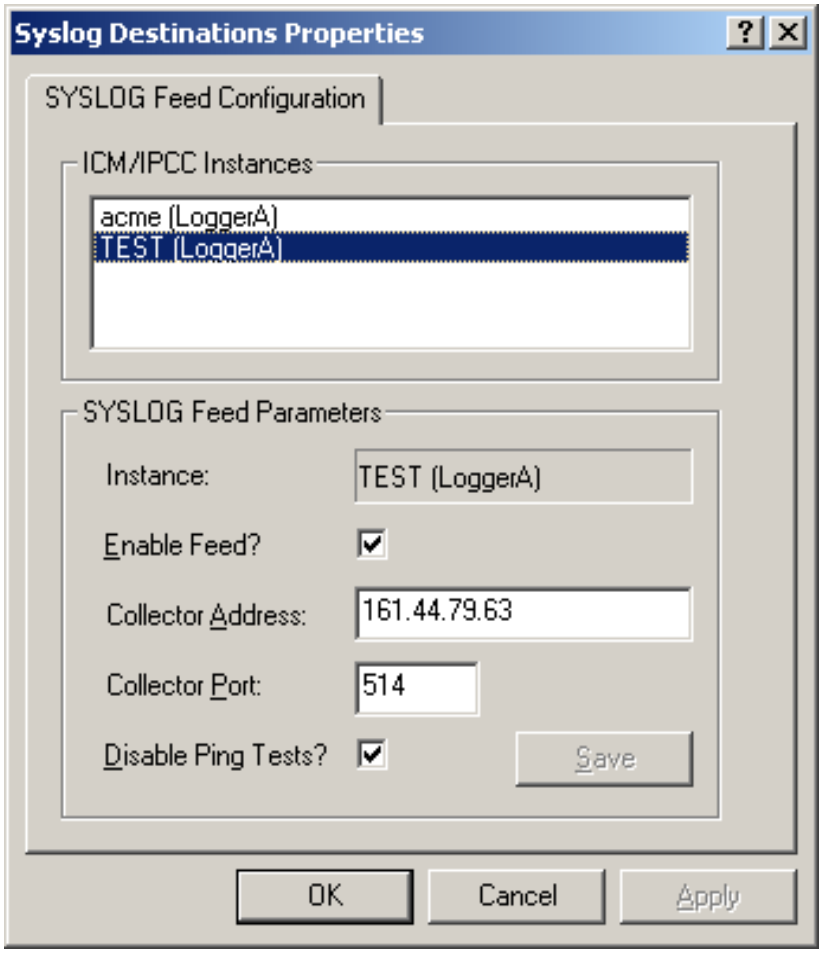


Figure 21: syslog Feed Configuration Dialog Box

IMPORTANT: You must cycle the Logger service to start the flow of events from the syslog feed. The Node Manager picks up the configuration parameters from the registry and passes them to the CW2KFEED process when it invokes it. Changing the syslog parameters and killing the CW2KFEED process cannot suffice because the Node Manager restarts it with the parameters it previously read from the registry. A service recycle is required.

6 Unified ICM/Unified CCE Services and Processes

Each Unified ICM/Unified CCE component consists of one or more processes, which are enabled and managed by Node Manager. Each component has a separate Node Manager that is installed as a Windows service. All Node Manager services have the same process name, *nodeman.exe*.

6.1 Services

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

Key Definition	Description
Critical:	This process is critical to the operation of the component. Failure of the process renders the Contact Center 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 Contact Center 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 6-1: Unified ICM/Unified CCE Processes

Component	Process	Description
Router	* router.exe	[Critical]: This is the primary Router process.
	* rtsvr.exe	[Critical]: Provides real-time data feed from the Router to the Administration & Data Server.
	* mdsproc.exe	[Critical]: Message Delivery Service
	* ccagent.exe	[Critical]: Router component that manages communication links between the Router and peripheral gateways.
	* dbagent.exe	[Critical]: Manages connections and transactions (configuration updates) from configuration tools.
	* testsync.exe	[Non critical] Provides interface for component test tools.
	* appgw.exe	[Optional/Critical]: The process that provides an interface for the Router to communicate with external applications.
	* dbworker.exe	[Optional/Critical]: The process that provides the interface for the Router to query external databases.

Component	Process	Description
	* [NIC].exe	[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, cainnic.exe, netwrkcic.exe, crspnic.exe, cwcnic.exe, gktmpnic.exe, incrpnic.exe, mcinic.exe, gennic.exe, ntnic.exe, ntlnic.exe, sprnic.exe, ss7innic.exe, stentornic.exe, timnic.exe, unisourcenic.exe
Logger	* configlogger.exe	[Critical]: The process that manipulates configuration data.
	* histlogger.exe	[Critical]: The process that inserts historical data into TMP historical tables in the Logger database.
	* recovery.exe	[Critical]: This process bulk copies historical data from the TMP historical tables to the actual historical tables. Recovers and synchronizes historical data with its partner logger during failover if loggers are running duplex. In addition, it is responsible for historical data purges in the Logger database based on configured retention parameters.
	* replication.exe	[Critical]: The process that replicates data from the Logger to the Historical Data Server on an Administration & Data Server.
	* csfs.exe	[Critical]: The alarm/event processor. CSFS distributes alarms/events send via EMS to supported alarm/event feeds, for example, SNMP, syslog. CSFS stands for Customer Support Forwarding Service, which in Unified ICM's infancy, forwarded events to a central monitoring location.
	* cw2kfeed.exe	[Optional]: The syslog event feed. This process acquires events from the CSFS process, formats them appropriately in accordance with the Berkley syslog protocol and sends the events to the configured collector. If a syslog collector is not configured, this process does not execute.
	* campaignmanager.exe	[Optional/Critical]: Outbound Option Campaign Manager. This process manages customer lists: provides customer records for every Dialer in the enterprise; determines when customers should be called again; maintains the "Do Not Call" list in memory. The Campaign Manager also sends real time and historical data to the Router and distributes configuration information to Dialer and Import processes. This process is installed and executes on the "A" side Logger only.
	* baimport.exe	[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

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

Component	Process	Description
		PIM.
	* ctiosservernode.exe	[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.
	* jtapigw.exe	[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.
	* ctisvr.exe	[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.
	IPPASvr.exe	[Optional/Critical] Cisco Agent Desktop: Cisco Browser and IP Phone Agent Service
	FCCServer.exe	[Optional] Cisco Agent Desktop: Cisco Chat Service
	CTI Storage Server.exe	[Optional/Critical] Cisco Agent Desktop: Cisco Enterprise Service
	LDAPmonSvr.exe	[Optional/Critical] Cisco Agent Desktop: Cisco LDAP Monitor Service
	LRMServer.exe	[Optional/Critical] Cisco Agent Desktop: Cisco Licensing and Resource Manager Service
	RPServer.exe	[Optional/Critical] Cisco Agent Desktop: Cisco Recording & Playback Service
	FCRasSvr.exe	[Optional/Critical] Cisco Agent Desktop: Cisco Recording and Statistics Service
	DirAccessSynSvr.exe	[Optional/Critical] Cisco Agent Desktop: Cisco Sync Service
	FCVoIPMonSvr.exe	[Optional/Critical] Cisco Agent Desktop: Cisco VoIP Monitor Service
	slurpd.exe	[Optional/Critical] Cisco Agent Desktop: Directory Replication Service
	slapd.exe	[Optional/Critical] Cisco Agent Desktop: Directory Services
	tomcat5.exe	[Optional/Critical] Cisco Agent Desktop: Tomcat Service
	* badialer_ip.exe	[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.
Administration	* configlogger.exe	[Critical]: Processes inbound configuration data.

Component	Process	Description
& Data Server (AW/HDS)	* updateaw.exe	[Critical]: Updates the local configuration database with configuration data from the central controller.
	* rtclient.exe	[Critical]: Receives a real-time data feed (from a real-time distributor) and updates the local database.
	* rtdist.exe	[Critical]: Manages inbound real-time data from the real time server on the Router and distributes it to real-time clients.
	* replication.exe	[Critical]: Manages replicated historical data received from the Logger (HDS only) and inserts historical data in the HDS database. In addition, it is responsible for historical data purges in the HDS database based upon configured retention parameters.
	* cmsnode.exe	[Optional]: Configuration Management System (CMS). Manages configuration data for the ConAPI interface. This is a necessary interface (process) for the System CCE web configuration and the Agent Reskilling Tool. 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.
	* cms_jserver.exe	[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.
	tomcat5.exe	[Optional/Critical]: Apache Tomcat servlet engine for SCCE web config.
	* iseman.exe	[Optional]: Internet Script Editor
	sqlservr.exe	[Critical]: Microsoft SQL server process
	sqlmangr.exe	[Critical]: Microsoft SQL server process
	sqlagent.exe	[Optional]: Microsoft SQL server process
All Nodes	nodeman.exe	[Critical]: Node Manager. This process monitors the status of all Unified ICM/Unified CCE processes on the server; should a process terminate unexpectedly, the Node Manager automatically restarts that process.
	nmm.exe	[Critical]: Node Manager Manager. This process monitors the primary Node Manager (nodeman.exe) process; should the primary Node Manager (nodeman.exe) process terminate unexpectedly, the Node Manager Manager restarts it.
	snmpdm.exe	[Important]: SNMP master agent

Component	Process	Description
	cccsnmpmgmt.exe	[Important]: SNMP agent management service – this service manages the SNMP agent infrastructure and restarts any agents that may terminate unexpectedly. It also ensures that the agent processes run at a reduced priority so as to not adversely impact server performance.
	msnsaagt.exe	[Important]: Microsoft native subagent adapter
	hostagt.exe	[Important]: HOST-RESOURCES-MIB subagent
	sappagt.exe	[Important]: SYSAPPL-MIB subagent
	cccaagent.exe	[Important]: CISCO-CONTACT-CENTER-APPS-MIB subagent

6.2 Using the Local Desktop

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

6.3 ICM Service Control and Windows Task Manager

The Unified ICM Service Control displays the Node Manager service for each Unified ICM/Unified CCE component as well as its state and startup settings. Each Node Manager service appears in the following format: **Cisco ICM <instance> <component>**. As an example, the Unified ICM Service Control window shown below 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**.

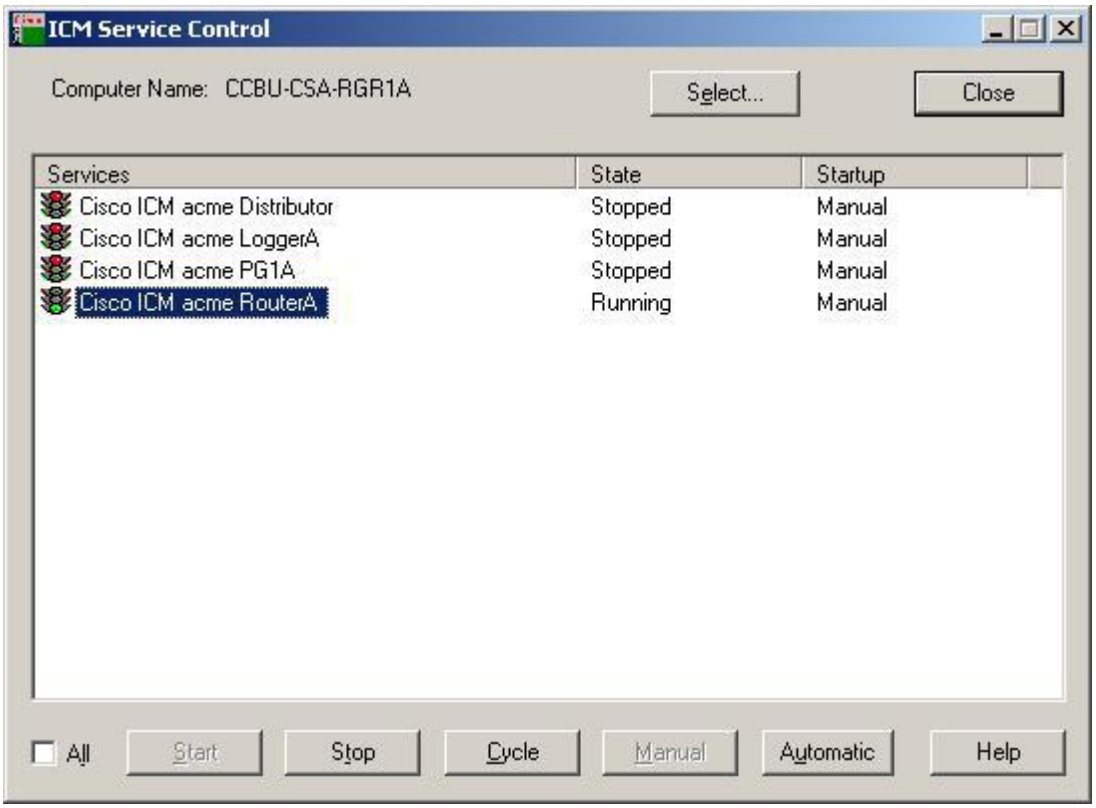


Figure 22: ICM Service Control

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 section 10.1.4.3 Accessing the Diagnostic Framework via the built-in User Interface (Portico).

6.4 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, you need to 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 process will be started and managed by the RouterA Node Manager process.

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

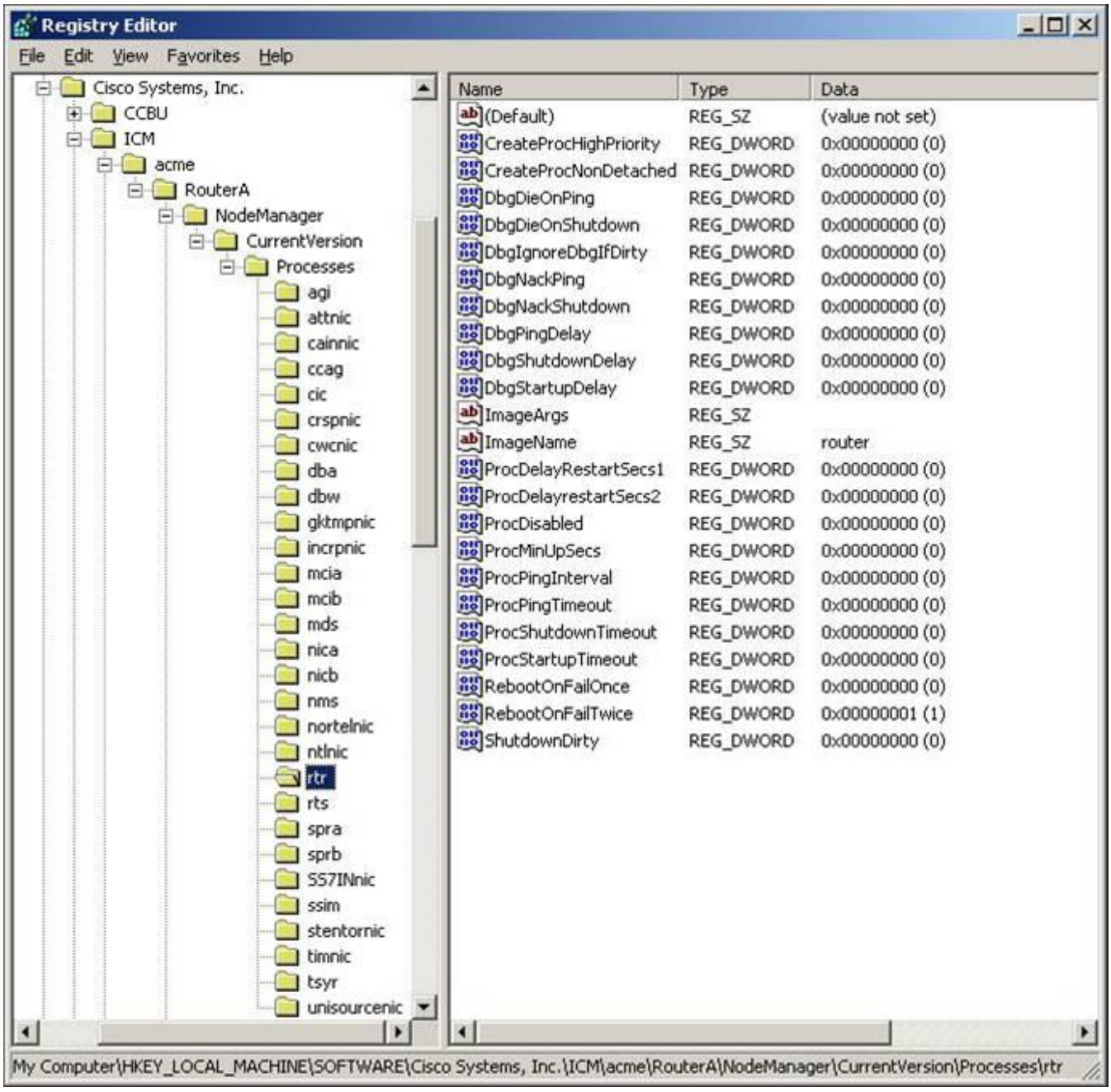


Figure 23: Registry Editor

6.5 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 *ccaComponentElmtRunID* value, which is the process ID, is valid if the *ccaComponentElmtStatus* is active, started, or standby.

cccaInstanceName.0 = acme
cccaComponentType.0.1 = router(1)
cccaComponentName.0.1 = RouterA
cccaComponentStatus.0.1 = started(4)
cccaComponentElmtName.0.1.5 = router
cccaComponentElmtRunID.0.1.5 = 4040
cccaComponentElmtStatus.0.1.5 = active(5)

The next example shows the entries for *acme-LoggerA*, the configlogger process. The *ccaComponentElmtRunID* value, which is the process ID, is valid if the *ccaComponentElmtStatus* 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)

7 Unified ICM/Unified CC Trace Levels

With serviceability enhancement, Unified ICM and Unified Contact Center application Release 8.0 utility tools provide centralized control for setting up each component trace level. You can also manually modify it from the registry key settings.

Users can either use the tool or manually modify the registry key value.

Unified ICM and Unified Contact Center application components write trace messages to trace log files on the local disk; these traces provide the following details about the operation of the component:

1. Error conditions (errors that may impair operation or performance are also reported in the Windows Event Log and sent via the syslog feed or, if sufficiently actionable, as SNMP notifications)
2. Debugging messages (to be used by troubleshooting engineers to diagnose problems)
3. Periodic performance metrics
4. Call state and/or call progress information
5. Configuration parameters or errors
6. Connectivity information (details about successful and failed connections)

The level of detail that is written to these trace logs can be controlled via numeric settings in the registry or via tools that interact directly with the application component to control tracing. The default settings (upon installation of the component) seek to balance performance with tracing detail with the scale tipped toward maximizing performance. Any increase in tracing levels has a corresponding adverse impact on performance (for example, agent capacity, IVR port capacity, inbound call load capacity) as additional computing resources are then consumed by the resulting disk I/O.

The amount of tracing that is stored on the local disk is controlled by the tracing infrastructure; a sliding (fixed size) window of tracing is maintained whereby the oldest data is deleted to make room for the newest data. You can control the size of this window by carefully editing parameters in the Windows registry. The tracing window size is represented in bytes (disk consumption), not by a time duration.

Routine capacity utilization measurements indicate the amount of computing resources that are available for added diagnostics (for more information, see section 9 Capacity Planning). If the deployment is already at high utilization, you must take care to understand the impact of enabling additional tracing to ensure that doing so does not adversely impact normal operation.

Before enabling additional tracing, Cisco recommends that you monitor the Health Monitoring Performance Counters while the tracing change is in effect to ensure that the server is not exceeding maximum thresholds. For more information, see section 8.1 Platform Health Monitoring Counters.

What follows is the recommended trace settings you must configure when you initially engage in diagnosing a problem. TAC may suggest some differences based upon their initial impressions of the problem symptoms. These are proposed for those who wish to take a quick, proactive approach in getting the trace levels up as quickly as possible to gather as much useful information as soon as possible.

Remember that TAC or BU engineers very likely may come back with additional settings based upon their initial log analysis.

Do not set what you believe to be maximum tracing – doing so could cause more problems than you had initially or even mask the problem by significantly changing timing.

7.1 Trace levels

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

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

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

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/set trace level and collect trace files are supported only for the following processes.

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

7.1.1 Trace–All Nodes

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

The Diagnostic Framework does not support the Administrator Workstation.

7.1.2 Trace–Administration and Data Server (previously known as the Distributor Administrator Workstation)

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

CMSNODE	0x00	0x00	0x00	0xFFFFFFFF
CMS_JSERVER	0x00	0x00	0x00	0xFFFFFFFF
REPLICATION	0x00	0x0F	0xFF	0xFFF
RTCLIENT	0x00	0x0F	0xFF	0xFFF
RTDIST	0x00	0x0F	0xFF	0xFFF
UPDATEAW	0x00	0x0F	0xFF	0xFFF
ISEMAN	0x00	0x00	0x00	0x01

7.1.3 Trace–Router

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

7.1.4 Trace–Logger

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
BAIMPORT	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF
CAMPAIGN MANAGER	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF
CONFIGLOGGER	0x00	0x0F	0xFF	0xFFF
CSFS	0x00	0x00	0x00	0xFF
CW2KFEED	0x00	0x00	0x00	0x07

DTP	0x00	0x04	0x06	0x0F
HISTLOGGER	0x00	0x0F	0xFFF	0xFFF
RECOVERY	0x00	0x0F	0xFFF	0xFFF
REPLICATION	0x00	0x0F	0xFFF	0xFFF

7.1.5 Trace–Peripheral Gateway

Process	**Level 0** **(Default - Error)**	**Level 1** **(Warning)**	**Level 2** **(Informational)**	**Level 3** **(Debug)**
JTAPIGW *	JT_JTAPI_EVENT_ USED JT_TPREQUESTS JT_PIM_EVENT JT_ROUTE_ MESSAGE	JT_CONNECTION *CONF*	JT_JTAPI* JT_HEX JT_ROUTE* JT_TERM* JT_LOW*	JT*
MDSPROC	0x00	0x07	0x0F	0xFF
MSGIS	0x00	0x00	0x00	0x3F
OPC **	default, cstacer EMSTraceMask = 0x40	agent, inrcmsg, closedcalls, tpmsg, routing EMSTraceMask = 0x40 Note: Remove "default" tracing set in Default(0) level, but include cstacer.	calls, NCT, simplified EMSTraceMask = 0x40 Note:Remove "default" tracing set in Default(0) level, but include Level 1.	Missingdata, halfhour EMSTraceMask = 0x40 Note: Remove "default" tracing set in Default(0) level, but include Level 2.
PGAGENT	0x00	0x03	0x0F	0xFF
EAGTPIM *	tp* precall *event csta* call_object teld_agent_state opcrequest	periph* jtapi_dialed*	autoconfig* teld* call_match_timing timer*	lock* universal* service* threadid jtapi*
VRUPIM	EMSTraceMask= 0x0 EMSUserData= 0x71f7e0	EMSTraceMask= 0x0 EMSUserData= 0x71f7e0 00000000000000000000 00000000000000000000 0000000000000000	EMSTraceMask= 0x0 EMSUserData= 0x71f7e0 00000000000000000000 00000000000000000000 0000000000000000	EMSTraceMask= 0x0 EMSUserData= 0xf1fff0 00000000000000000000 00000000000000000000 0000000000000000

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
		0000 000000000180	000 000000000180	00 000000000000180
ACMIPIM	EMSUserData = (hex) 01, 7f, 46, 00, 00, 00, 00, 00, 00, 00, 00, 01, 00, 00, 00, 00, 00, 3f, ff, ff, ff, 67, cf, d7, fd, ef, ff, ff, ff, ff, ff, ff, ff, ff, ff, ff, f0, fa For reference, this is the default + all_peripherals	EMSUserData = (hex) f5, 7f, 46, 00, 00, 00, 00, 00, 00, 00, 00, 01, 00, 00, 00, 00, 00, 3f, ff, ff, ff, 67, cf, d7, fd, ef, ff, ff, ff, ff, ff, ff, ff, ff, ff, ff, f0, fa For reference this is level 0 + timer events	EMSUserData = (hex) f5, 7f, c6, 00, 00, 00, 00, 00, 00, 00, 00, 01, 00, 00, 00, 00, 00, 3f, ff, ff, ff, 67, cf, d7, fd, ef, ff, ff, ff, ff, ff, ff, ff, ff, ff, ff, f0, fa For reference this is level 1 + Monitor Item traversal	EMSUserData = (hex) f5, 7f, f6, 00, 00, 00, 00, 01, ff, ff, fe, c1, 00, 00, 00, 00, 00, 3f, ff, ff, ff, 67, cf, df, fd, ef, ff, ff, ff, ff, ff, ff, ff, ff, ff, ff, ff, fe For reference this is level 2 + locks + socket data
ARSPIM *	tp* precall *event csta* call_object teld_agent_state opcrequest	periph*	autoconfig* teld* call_match_timing timer*	lock* universal* service* threadid
MRPIM	EMSUserData = 0x00 Procmon: > trace mr* /off	EMSUserData = 0x40 Procmon: > trace mr* /off > trace mr_msg_comm_session /on	EMSUserData = 0x58 Procmon: > trace mr* /off > trace mr_msg_comm_session /on > trace mr_*_mr /on	EMSUserData = 0x5F Procmon: > trace mr* /off > trace mr_msg_comm_session /on > trace mr_*_mr /on > trace mr_*_inrc /on > trace mr_*_csta /on
CTISRVR	0x000000f0	0x000000f6	0x000000fe	0x000000ff
CTIOS SERVER NODE	0x00060A0F	0x00240A2F	0x00260A2F	0x002E0A2F
BADIALER	EMSTraceMask= 0x0000001f EMSUserData=0xFFFF	EMSTraceMask= 0x0000003f EMSUserData= 0xFFFF	EMSTraceMask= 0x0000007f EMSUserData= 0xFFFF	EMSTraceMask= 0x000000ff EMSUserData= 0xFFFF

7.1.6 Trace–Web Setup

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

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

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

7.1.7 Trace–Diagnostic Framework

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

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

7.2 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

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

File compression is activated for the supported PG components when:

- You install one of the following patches:
  - 7.5(10)
  - 8.0(3)
  - 8.5(1)
  - 8.5(2)
- You run PG setup on PGs with the supported PG components.

File compression is activated on the CTI OS Server when:

- You install one of the following patches:

- 7.5(10)
- 8.0(3)
- 8.5(1)
- 8.5(2)

- You run CTI OS Server setup.

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

7.2.1 Patch Installer - New Default Value for EMSAllLogFilesMax

For the components that support EMS file compression, EMSAllLogFilesMax is set to 2 GB if the install drive has at least 25 GB free disk space. The new value is set when you install the patch is or when run PG or CTI OS Server setup on the supported components. The new default value of this registry key allows up to 2 GB of logs to be maintained (size taken post compression) on the system.

7.2.2 CTI OS Setup Information post patch

When you run the patch installer, EMSAllLogFilesMax is set to 2 GB as mentioned above. When you run the CTI OS Server setup, EMSAllLogFilesMax is unconditionally set to 2 GB.

7.2.3 Dumplog

Dumplog was updated to handle 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. If you must dump logs from compressed EMS files (with .gz extension) outside of a PG or CTI OS Server, the EMS files can be unzipped before using dumplog.

7.2.4 EMS File Compression Control

To enable or disable compression of EMS log files, the EMSZipCompressionEnabled registry key in \EMS\CurrentVersion\Library\Processes\<process name> is used. Cisco recommends that you do not modify this registry key. This key takes effect only on components that support EMS file compression.

7.2.5 Other registry keys

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

- EMSZipFormat
- EMSZipExtension

Note: *Do not* modify these registry keys.

7.3 How to Set Router Tracing

To set the Unified ICM/CCE Router, use the Router Trace utility. This is a single-form Windows GUI utility that is loaded on the Unified ICM/Unified CCE server. To launch the utility, connect to the server through a remote desktop (or go to the local console); invoke RTRTRACE from ICM\BIN:

C:> \icm\bin\rtrtrace

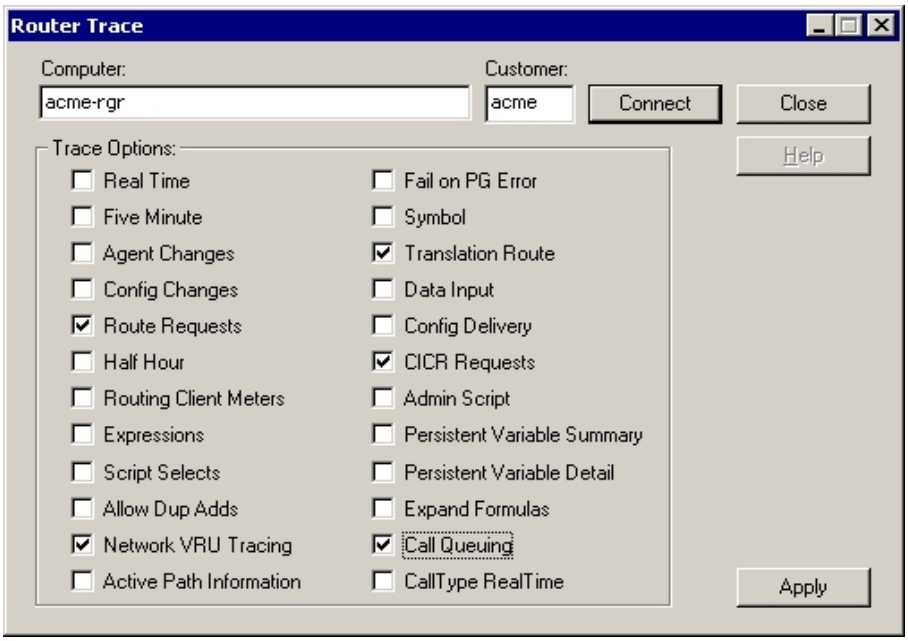


Figure 24: Router Trace Utility

When a call routing failure occurs, the basic traces should at the minimum be "Route Requests" and "Translation Route" (if translation routing is used).

Additionally, the other tracing should be enabled depending on the specific problems seen.

Table 7-1: Setting Router Tracing

For any type of VRU	enable "Network VRU Tracing"
For NAM-CICM (Hosted)	enable "CICR Requests"
For suspected queuing issues	enable "Call Queuing"
For Call Type Reporting Problems	enable "Call Type Real Time"
For Agent Issues	enable "Agent Changes"

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 very useful.

7.4 How to Set OPC Tracing

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

Command Syntax (launch):

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

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

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

Cisco recommends the following commands to alter default trace levels. Cisco recommends that you first understand your current utilization to ensure there is sufficient capacity to accommodate the added tracing.

7.4.1 General Diagnostics

```
opctest:debug /on
```

7.4.2 Diagnosing Network Transfer Issues

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

7.4.3 Diagnosing Multi Media Issues

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

7.4.4 Diagnosing VRU PG Issues

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

The default is:

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

and

```
EMSTracemask = 0x40
```

EMSTracemask is reset in the Windows registry.

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

7.4.5 How to Restore Default Trace Levels

```
opctest:debug /on
```

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

7.4.6 How to Display Trace Levels

```
opctest:debug /showtrace
```

This parameter displays current trace levels enabled on the peripheral.

7.5 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 7-2: Setting Unified CCM PIM Tracing

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

7.5.1 ARS Gateway Registry Trace Settings

Table 7-3: Setting ARS Gateway Registry Tracing

Registry Key	**HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\ARSGW\ EMS\CurrentVersion\Library\Processes\arsgw1\EMSTraceMask**
Item	**EMSTraceMask**
Value	**0x80023fff** The value of **0x80023fff** provides sufficient tracing information to troubleshoot most issues.
Registry Key	**HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\ARSGW\ EMS\CurrentVersion\Library\Processes\PG\CurrentVersion\ARS\ARSgw1\ARSData\Dynamic\EMSTraceMaskCollectMsg**
Item	**EMSTraceMaskCollectMsg**
Value	**0xffffffff** The value of **0xffffffff** provides sufficient tracing information to troubleshoot most issues.

7.5.1 ARS PIM Trace Settings

Table 7-4: Setting ARS PIM Tracing

Command Syntax (launch)	**C:> ProcMon <*instance*> <*node*> pim<*pim number*>**
Example	**C:> ProcMon acme PG1A arspim1**

Commands	**debug /level 2**

7.6 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 7-5: Setting JTAPI Gateway Tracing

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

7.6.1 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.

7.7 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 7-6: Setting CTI Server Tracing

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

7.7.1 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.

7.8 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 7-7: Setting CTI Server Tracing

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

7.9 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 7-8: Setting VRU PIM Tracing

Registry Key	**HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\PG<PG number><A or B>\EMS\CurrentVersion\Library\Processes\pim<pim number>**
Example	**HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\acme\PG2A\EMS\CurrentVersion\Library\Processes\pim1**
Item	**EMSUserData**
Value	**7F F7 E0 (hex)**

Item	**EMSTraceMask**
Value	**0 (zero)**

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

\icm\<*inst*>\<pg><pg number><a or b>\vrucap

For example: **\icm\acme\pg2a\vrucap**

7.9.1 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

7.10 Setting Outbound Option Tracing

The Release 8.0(1) utility tools provide centralized control to set up each component trace level. Additionally, you can manually modify the registry key values.

7.10.1 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.\ICM\m3pc1\LoggerA\EMS\CurrentVersion\Library\Processes\CampaignManager

7.10.2 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:

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

Example:

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

7.10.3 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

7.11 Setting Trace File Retention Parameters

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:

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

Example:

C:\icm\acme\pg1a\logfiles

Trace log files are in the following format:

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.

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

Table 7-9: Registry Items

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.

8 Performance Counters

8.1 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.

Table 8-1: Performance Counters - Health Monitoring

Performance Object	Counter Name (Instance)	Type	Units (Range)	Threshold Green	Threshold Yellow	Threshold Red
Processor	% Processor Time (_Total)	Int32	Percentage (0 - 100%)	< 50%	50% - 60%	> 60% (sustained)
Primary indicator of processor activity; displays the average percentage of CPU busy time observed during the sample interval.						
System	Processor Queue Length	Int32	# threads	< 2 * #CPUs	-	>= 2 * #CPUs (sustained)
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.						
Memory	Available Bytes	Int32	Percentage (0 - 100%)	> 30%	20% - 30%	< 20%
Amount of physical memory available to running processes; threshold values are a percentage of physical memory. This is a snap shot–not a running average. Sustained samples below 20% (available) may be indicative of a memory leak.						
Memory	Pages / sec	Int32	# page faults	< 10	>= 10	> 10 (sustained)
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.						
Physical Disk	Avg. Disk Queue Length (_Total)	Float	Average # read/write requests	< 1.5	-	>= 1.5 (sustained)
Average number of both read and write requests that were queued for the selected disk during the sample interval.						
Physical Disk	% Disk Time (_Total)	Int32	Percentage (0 - 100%)	< 60%	60% - 80%	> 80%
Percentage of elapsed time that the disk drive was busy servicing read or write requests.						
Network Interface	Bytes Total/sec	Int32	Percentage (0 - 100%)	< 25%	25% - 30%	> 30%
Rate at which bytes are sent and received over each network adapter. Threshold values are a percentage of available bandwidth.						
Network Interface	Output Queue Length	Int32	# packets in queue	0	1	> 1 (sustained

						)
Length of the output packet queue (in packets). If too large, there are delays and the bottleneck should be found and eliminated.						
SQLServer:Buffer Manager	Buffer cache hit ratio	Int32	Percentage (0 - 100%)	> 90%	-	< 90%
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 recommended 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.						

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.

8.2 Platform Diagnostic Counters – Automatic Collection

The following counters values are sampled and collected automatically (by the Node Manager):

- Counter values are stored in a disk file on the server.
- Counter values are sampled at a "one minute" interval.
- Data files contain a rolling window of counter values – older data is discarded in lieu of new data. Data is stored in multiple files (maximum size is 1 MB each) and a maximum of 45 days of data is saved.

Table 8-2: Platform Diagnostic Counters Values

Data file location	**\icm\log**
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 8-3: Performance Counters - Diagnostics

Component	Counter Name	Type	Units (Range)
Processor	% Processor Time (_Total)	Int32	Percentage (0 – 100%)
% 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 of 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%.			

Process	Handle Count (_Total)	Int32	# handles
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.			
Memory	Page Faults / sec	Int32	# faults
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.			
Memory	Committed Bytes	Int32	# bytes
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.			
Memory	Pages / sec	float	# pages per second
Pages/sec is the rate at which pages are read from or written to disk to resolve hard page faults. This counter is a primary indicator of the kinds of faults that cause system-wide delays. It is the sum of Memory\\Pages Input/sec and Memory\\Pages Output/sec. It is counted in numbers of pages, so it can be compared to other counts of pages, such as Memory\\Page Faults/sec, without conversion. It includes pages retrieved to satisfy faults in the file system cache (usually requested by applications) non-cached mapped memory files.			
System	Threads	Int32	# threads
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.			
System	Processor Queue Length	Int32	# threads
Processor Queue Length is the number of threads in the processor queue. Unlike the disk counters, this counter 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 need to divide this value by the number of processors servicing the workload. A sustained processor queue of less than 10 threads per processor is normally acceptable, dependent of the workload.			
System	Processes	Int32	# processes
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.			

8.3 Platform Diagnostic Counters

8.3.1 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 8-4: Diagnostic Counters - All Components

Performance Object	Instance	Counter Name
LogicalDisk	_Total	Avg. Disk Queue Length
LogicalDisk	C:	Avg. Disk Queue Length
LogicalDisk	<DB Drive>	Avg. Disk Queue Length
Network Interface	<NIC Name>	Packets Outbound Discarded
PhysicalDisk	_Total	Disk Transfers / sec
Process	_Total	Page Faults / sec
Process	_Total	Virtual Bytes
Process	_Total	Working Set
Processor	_Total	Interrupts / sec
Process	<virus scanner>	% Processor Time
Process	<virus scanner>	Page Faults / sec
Process	<virus scanner>	Virtual Bytes
Process	<virus scanner>	Working Set

8.3.2 Logger/Administration & Data Server/HDS

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

Set the initial sample frequency to 15 seconds. If not sufficient resolution, decrease to a 5 second interval.

Table 8-5: Diagnostic Counters - Logger, Administration & Data Server, and HDS

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

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

AW/HDS Processes: configlogger, recovery, replication, rtclient, rtdist

8.3.3 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 8-6: Diagnostic Counters - SQL Server

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

[1] Where "csco" is the Unified ICM/Unified CCE instance name.

8.4 Component-Specific Counters

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

8.4.1 Router

Table 8-7: Router Performance Counters

Performance Object: Cisco ICM Router		
Counter Instance: "{ICM Instance Name}" – if multiple instances installed		
Always ON?	**Counter Name**	**Description**
Y	Agents Logged On [1]	The number of (contact center) agents currently logged in.

Y	Calls In Progress [1]	The number of calls currently in progress (being controlled by the CCE application).
Y	Calls/sec [1]	The (calculated) inbound call rate measured in the number of calls received per second.
Y	Calls In Queue	The number of calls queued in all network Voice Response Units (VRUs), from the Router's perspective, including those calls that are in the process of transferring to the VRU for queuing.
Y	Calls In Router	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.
N	Router State Size	The current Router state size - the total size of all of the state transfer objects in Router memory; this size is measured in kilobytes. After one Router side goes out of service, when it returns in-service, the Router state is transferred from the surviving Router side to the returning Router side.
N	Messages Processed/sec	The number of MDS messages Router processed. By default, this counter is disabled.
N	Bytes Processed/sec	The rate of the data bytes the Router processed. By default, this counter is disabled.
N	Avg Process Time/Message (ms)	The average time (in milliseconds) the Router spends processing a MDS message.
N	Max Process Time(ms)	The maximum time (in milliseconds) the Router spends processing a MDS message.

[1] These counters are also quite useful for long-term trending to determine whether there are capacity issues now or whether there are in the future. The counter values can be compared to other PerfMon counters (for example, CPU, Memory, Disk, and NIC). Relationships and cause/effect analysis can greatly assist in confirming existing or predicting upcoming capacity/performance problems.

To 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

8.4.2 Logger

Table 8-8: Logger Performance Counters

Performance Object: Cisco ICM Logger		
Counter Instance: "{ICM Instance Name}" – if multiple instances installed		
Always	**Counter Name**	**Description**

ON?		
Y	Number of DB Write Records	The number of database writes (records/rows) in the historical logger process that is written to the database at the time the counter is polled.
Y	DB Write Average Time	The average database write time expresses the average amount of time, in 100 nanosecond units, required to write data to a table in the central controller database. This value represents the average time per write of the write operations that occurred in the past second. This object is a good indicator of contention for database access.
Y	DB Write Records Processed	The number of records processed – written to the database – in the Historical Logger Process in the past second.

8.4.3 Administration & Data Server

Table 8-9: Administration & Data Server Real-time Counter

Performance Object: Cisco ICM Distributor RealTime		
Counter Instance: {Instance Name} ADS#		
Always ON?	**Counter Name**	**Description**
Y	Agent Queue Depth	The queue depth – number of pending write transactions – for the Agent table in the Real-time Client process.
Y	Agent DB Write Average Time	The average time – in units of 100 ns – for the Real-time Client process to write an Agent table transaction within the past 1 second interval.
Y	Agent DB Write Records Processed	The number of Agent table records written by the Real-time Client process in the past 1 second interval.
Y	Agent Skill Group Queue Depth	The queue depth – number of pending write transactions – for the Agent Skill Group table in the Real-time Client process.
Y	Agent Skill Group DB Write Average Time	The average time – in units of 100 ns – for the Real-time Client process to write an Agent Skill Group table transaction within the past 1 second interval.
Y	Agent Skill Group DB Write Records Processed	The number of Agent Skill Group table records written by the Real-time Client process in the past 1 second interval.
Y	Skill Group Queue Depth	The queue depth – number of pending write transactions – for the Skill Group table in the Real-time Client process.
Y	Skill Group DB Write Average Time	The average time – in units of 100 ns – for the Real-time Client process to write an Skill Group table

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

Table 8-10: Administration & Data Server Replication Counters

Performance Object: Cisco ICM Distributor Replication		
Counter Instance: {Instance Name} Distributor #		
Always ON?	**Counter Name**	**Description**
Y	DB Write Average Time	The average time – in units of 100 nanoseconds – for database write operations in the HDS Replication process during the past 1 second interval.
Y	DB Write Records Processed	The number of records written by the HDS Replication process in the past 1 second interval.

8.4.4 PG – OPC

Table 8-11: PG - OPC Counters

Performance Object: **Default**: Cisco ICM OPC **Optionally Enabled**: Cisco ICM OPC (Optional)		
Counter Instance: "{Instance Name} PG#A/B" (For example, "acme PG3A")		
Always ON?	**Counter Name**	**Description**
Y	Call Count	Number of Calls that are currently active.
N	Agent Count	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.
N	Skill Group Count	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.
N	Services Count	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.
Y	Logged-In Agent Count	This counter gives the number of agents that have logged in. This does not necessarily indicate that the agents are ready to accept calls.
Y	Ready Agent Count	Number of Agents that are logged in and are ready to accept calls.
N	Not-Ready Agent Count	Number of Agents that are logged in, but occupied with task other than accepting incoming calls.
Y	Talking Agent Count	Number of Agents currently talking on Inbound or Outbound calls.
N	Held Agent Count	Number of Agents that are inactively participating in a call.
N	Work-Ready Agent Count	Agents occupied with work associated with the last call. This implies that agent is no longer connected to the call and is ready to receive additional calls when they exit this state.
N	Work-Not-Ready Agent Count	Agents occupied with work associated with the last call. This implies that agent is no longer connected to the call. These Agents are not ready to receive additional calls

		when they exit this state.
N	Logged-Out Agent Count	Number of Agents that are logged out of the system. This count helps in validating the statistics if there are any state mismatches.
N	None-State Call Count	This count gives the number of calls for which a call object was created but no activity.
N	Null-State Call Count	This count gives the number of calls that has no relationship between the call and device.
N	Initiated Call Count	This count gives the number of calls for which the device has requested for a service. Often this is the dialing state.
N	Alerting Call Count	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.
Y	Connected Call Count	This count gives the number of calls for which the device is actively participating in the call.
N	Held Call Count	This count gives the number of calls for which the device is inactively participating in the call.
N	Queued Call Count	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.
N	Failed Call Count	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.

To 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

8.4.5 PG – Communications Manager (EA) PIM

Table 8-12: PG - CM PIM Counters

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

To 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

8.4.6 PG – VRU PIM

Table 8-13: PG - VRU PIM Counters

Performance Object: Cisco ICM VRUPIM		
Counter Instance: "{Instance Name} PG#A/B PIM#" (For example, "acme PG3A PIM3")		
Always ON?	**Counter Name**	**Description**
Y	Calls At VRU	Calls at VRU is the number of calls that are currently at the Voice Response Unit (VRU). For a VRU that only uses a Call Routing Interface, this value is zero.
N	Messages To VRU/sec	Messages To VRU/sec is the rate at which messages are sent to the Voice Response Unit (VRU). This counter is active only when enabled in ICM registry.
N	Messages From	Messages From VRU/sec is the rate at which messages are

	VRU/sec	received from the Voice Response Unit (VRU). This counter is active only when enabled in ICM registry.
N	Bytes To VRU/sec	Bytes To VRU/sec is the rate at which bytes are sent to the Voice Response Unit (VRU). This counter is active only when enabled in ICM registry.
N	Bytes From VRU/sec	Bytes From VRU/sec is the rate at which bytes are received from the Voice Response Unit (VRU). This counter is active only when enabled in ICM registry.
Y	New Calls/sec	New Calls/sec is the rate at which new calls arriving at the Voice Response Unit (VRU). New calls are calls not under ICM script control when arriving at a Service Control VRU.
Y	Pre-Routed Calls/Sec	Pre-Routed Calls/sec is the rate at which Pre-Routed calls are arriving at Voice Response Unit (VRU). Pre-Routed calls are calls under ICM script control when arriving at a Service Control VRU.
Y	Connection Resets	Connection Resets is the number of times the TCP connection between ICM and the Voice Response Unit changed from an established state to a closed state since the application started.

To 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

8.4.7 CTI Server

Table 8-14: CTI Server Counters

Performance Object: **Default**: Cisco ICM CTISVR **Optionally Enabled**: Cisco ICM CTISVR (Optional)		
Counter Instance: "{Instance Name} CG#A/B" (For example, "acme CG3A")		
Always ON?	**Counter Name**	**Description**
N	Reported Call Count	Number of calls that are already reported to the CTI clients.
N	Active Call Count	Number of calls that are currently in progress.
N	Deactivated Call Count	Number of calls that are not currently active and eventually cleared.
N	Cleared Call Count	Number of calls that no longer exist in the system.
N	Private Call Count	Number of calls that are privately tracked by CTI Server and which are not reported to OPC.

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

To 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

8.4.8 CTI OS Server

Table 8-15: CTI OS Server Counters

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

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

		calls being completed by agents equals the call arrival rate.
N	CTI OS Argument Object Count	The total number of active CTI OS argument objects. This value shows how many CTI OS argument objects were created since it last started. This value shall be quite large, go up and down and may reach a steady state when the number of calls being completed by agents equals the call arrival rate.
N	CTI OS Device Object Count	The total number of active CTI OS devices. This value shows how many CTI OS device objects were created since it last started. This value should mainly stay constant while CTI OS runs.
N	CTI OS Agent Object Count	The total number of CTI OS agent objects. This value shows how many CTI OS agent objects were created since it last started. This value should stay constant while CTI OS runs unless agents are added or deleted.
N	CTI OS Skill group Object Count	The total number of CTI OS skill group objects. This value shows how many CTI OS skill group objects were created since it last started. This value should stay constant while CTI OS runs unless skill groups are added or deleted.
N	CTI OS Supervisor Object Count	The total number of CTI OS Supervisor objects. This value shows how many CTI OS supervisor objects were created since it last started. This value should stay constant while CTI OS runs unless supervisors are added or deleted.
N	CTI OS Team Object Count	The total number of CTI OS Team objects. This value shows how many CTI OS team objects were created since it last started. This value stays constant while CTI OS runs unless teams are added or deleted.
N	CTI OS Total Objects Created Count	The total count of all objects created by CTI OS. This value shows how many CTI OS objects were created since it last started. This value only increases and grows very large as CTI OS up time increases.
N	CTI OS Total Objects Deletion Count	The total count of all objects deleted by CTI OS. This value shows how many CTI OS objects were deleted since it last started. This value only increases and grows very large as CTI OS up time increases. It never equals the total objects created count as some objects are never deleted after being created by CTI OS like agent, device, team and skill group objects.
N	CTI OS Active Object Count	The total count of all objects created by CTI OS that are active. This value shows how many CTI

		OS objects are currently allocated since it last started. If this value begins to increase it would indicate that a memory leak is occurring in CTI OS. The specific object counters show which object is not being released.
Y	CTI OS CLIENT Send Message Rate (msg/sec)	The rate at which CTI OS sends messages to Clients per second. This value shows the number of messages, per second, that CTI OS is delivering messages to CTI OS desktops. As this value increases it indicates that CTI OS server is being placed under an increasing load. A review of the configuration as it relates to agents, skill groups and teams may be necessary.
Y	CTI OS CLIENT Receive Message Rate (msg/sec)	The rate at which CTI OS receives messages from Clients per second. This value shows the number of messages, per second, that are being received from the CTI OS desktops. As this value increases it indicates that CTI OS is being placed under an increasing request load from the desktops.
Y	CTI OS CLIENT Total Number of Pending Write Operations	The total number of pending write operations for all clients. This value shows the total number of messages in the system waiting to be read by CTI OS clients. If the value increases, it suggests that there are one or more clients not keeping up with reading messages from CTI OS.
Y	CTI OS CLIENT Total Message Buffer Size (Bytes)	The total number of bytes used to store the pending writes for all clients. This value shows the total amount of memory used to store all the messages that are waiting to be read by CTI OS clients.
Y	CTI OS CG Receive Queue Size	The number of messages queued in the CTI OS CG Receive Queue. This value is an indicator of the total load on the system. If it increases, a review of the configuration may be necessary to understand why CTI OS is not keeping up with the incoming message rate from the CTI Server.

To 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

8.4.9 Outbound Option Campaign Manager

Table 8-16: Outbound Option Campaign Manager Counters

Performance Object: Cisco ICM CampaignMgr		
Counter Instance: "{Instance Name}"		
Always ON?	**Counter Name**	**Description**
Y	DB Space Utilization	The Campaign Manager and Import processes share a private database on the Side A Logger. This shows what percentage of allocated space in the database is currently utilized. An administrator should start paying attention when this value exceeds eighty percent.
Y	Queue Depth	The Campaign Manager is a multithreaded process. There is one main dispatch thread that is involved in most processing. Queue Depth indicates how many messages are queued to this internal dispatch thread. By default, the Campaign Manager crashes when this value exceeds 10,000 messages in queue.
Y	Average Queue Time	The Campaign Manager is a multithreaded process. There is one main dispatch thread that is involved in most processing. This shows what is the average time spent in the main dispatch thread queue in milliseconds.
Y	Do Not Call Number Count	The Campaign Manager manages a global list of phone numbers used to prevent block dialing. This list is stored in memory. Each record uses 17 bytes of memory. This counter shows how many do not call entries are currently in memory.
Y	Active Dialer Count	The Campaign Manager process feeds several Dialer components which do all of the dialing of customers for outbound campaigns. This counter indicates how many Dialers are currently registered to the Campaign Manager.

8.4.10 Outbound Option Import

Table 8-17: Outbound Option Import Counters

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

8.4.11 Outbound Option Dialer

Table 8-18: Outbound Option Dialer Counters

Performance Object: Cisco ICM Dialer		
Counter Instance: "{Instance Name}"		
Always ON?	**Counter Name**	**Description**
Y	Queue Depth	The Dialer is a multithreaded process that communicates between threads using inter thread messaging. This indicates how many messages are currently queued up for the main dispatch thread. By default, the Dialer process restarts when this value exceeds 10,000 messages.
Y	Average Queue Time	The Dialer is a multithreaded process that communicates between threads using messaging. There is one main dispatch thread that is involved in most processing. This shows what is the average time spent in queue.
Y	Talking Agents	For an agent campaign, the Dialer replaces calls to customers and transfers those customers to agents. This counter indicates how many agents are currently talking in the monitored campaign skill group.
Y	Busy Port (Customer) Count	The port is the unit on the Dialer that places calls to reserve agents and to contact customers. This counter tracks how many ports are currently busy trying to contact customers.
Y	Busy Port (Reservation) Count	The port is the unit on the Dialer that places calls to reserve agents and to contact customers. This counter tracks how many ports are currently busy reserving agents.
Y	Idle Port Count	The port is the unit on the Dialer that places calls to reserve agents and to contact customers. This counter tracks how many ports are currently idle.
Y	Call Attempt Count	The Dialer attempts to contact customers and transfer them to reserved agents or an available IVR. This counter tracks how many customer attempts were placed today. It does not include preview calls that were rejected or skipped.
Y	Abandoned Call Count	When a customer is contacted and an agent is not available to take the call, the call can be dropped or sent to the IVR for prompting and queuing. When either of these conditions occurs, the 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.

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

8.4.12 Message Delivery Service

Table 8-19: MDS Client Counters

Performance Object: Cisco ICM MDSCLIENT		
Counter Instance: "{Instance Name}"		
Always ON?	**Counter Name**	**Description**
N	Client Handle ID	Handle for this MDS client. It is used to uniquely identify the MDS client connected to the MDS process.
N	Now Message Received	Number of messages received by the MDS client per second.
N	Now Message Sent	Number of messages sent by the MDS client per second.
N	Now Bytes Received	Number of bytes received by the MDS client per

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

Table 8-20: MDS Process Client Counters

Performance Object: Cisco ICM MDSPROCCLIENT		
Counter Instance: "{Instance name}"		
Always ON?	**Counter Name**	**Description**
N	Client Handle ID	Handle for this MDS client. It is used to uniquely identify the MDS client connected to the MDS process.
N	Total MDS Client Connects	Total number of times the MDS client has connected to the MDS process.

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

Table 8-21: MDS Process Counters

Performance Object: Cisco ICM MDSPROC		
Counter Instance: "{Instance Name}"		
Always ON?	**Counter Name**	**Description**
N	Current Buffers Memory Allocated	Total number of bytes used by all currently allocated buffers.
N	Current Buffers Allocated	Total number of buffers currently allocated from buffer pool.
N	Buffers Allocation Requests/sec	Number of buffers allocated per second.
N	Buffers Free Requests/sec	Number of buffers freed per second.

N	Current Buffers Memory Limit	Maximum amount of memory allowed to be allocated for buffers for this process.
N	Initial Buffers Memory Limit	Amount of memory limit reserved for buffers for this process.
N	Synch Messages Ordered/sec	Number of messages ordered by the MDS synchronizer per second.
N	Synch MDS Duplicates/sec	Number of duplicate MDS messages detected by the synchronizer per second.
N	Synch DMP Duplicates/sec	Number of duplicate DMP messages detected by the synchronizer per second.
N	LocalHighInQ Current Depth	Current number of messages in the Local High Incoming Queue.
N	LocalHighInQ Now Messages In/sec	Total number of messages added to the Local High Incoming Queue per second.
N	LocalHighInQ Now Messages Out/sec	Total number of messages removed from the Local High Incoming Queue per second.
N	LocalHighInQ Now Bytes In/sec	Total number of bytes added for all messages to the Local High Incoming Queue per second.
N	LocalHighInQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Local High Incoming Queue per second.
N	LocalHighInQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Local High Incoming Queue per second.
N	LocalHighInQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Local High Incoming Queue.
N	LocalHighInQ 90% Queue Response Time [ms]	The response time in milliseconds that 90% of all messages passing through the Local High Incoming Queue experience.
N	LocalMedInQ Current Depth	Current number of messages in the Local Medium Incoming Queue.
N	LocalMedInQ Now Messages In/sec	Total number of messages added to the Local Medium Incoming Queue per second.
N	LocalMedInQ Now Messages Out/sec	Total number of messages removed from the Local Medium Incoming Queue per second.
N	LocalMedInQ Now Bytes In/sec	Total number of bytes added for all messages to the Local Medium Incoming Queue per second.
N	LocalMedInQ Now Bytes Out/sec	Total number of bytes removed for all the messages from the Local Medium Incoming Queue per second.
N	LocalMedInQ Now Traffic Intensity	Ratio of the number of messages added to the number of messages removed from the Local Medium Incoming Queue per second.
N	LocalMedInQ Avg. Queue Response Time [ms]	Average time in milliseconds a message waits in the Local Medium Incoming Queue.

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

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

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

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

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

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

To enable optional counters:

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

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

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

Name: EnablePerformanceMonitor

Type: REG_DWORD

Default: 0 (disabled)

Enabled: 1

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

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

Name: EnablePerformanceMonitor

Type: REG_DWORD

Default: 0 (disabled)

Enabled: 1

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

8.4.13 QoS

Table 8-22: Cisco ICM QoS

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

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

N	Low LocalRttStdDev	Low LocalRttStdDev is the standard deviation of Round Trip Time of low priority messages as measured by local node.
N	Low RemoteRttMean	Low RemoteRttMean is the mean Round Trip Time in milliseconds of low priority messages as measured by remote node.
N	Low RemoteRttStdDev	Low RemoteRttStdDev is the standard deviation of Round Trip Time of low priority messages as measured by remote node.
N	Low Xmit NowQueueDepth	Low Xmit NowQueueDepth is the current number of messages in the transmit queue for low priority traffic.
N	Low Xmit MaxQueueDepth	Low Xmit MaxQueueDepth is the maximum number of message observed in the transmit queue for low priority traffic.
N	Low Xmit NowBytesQueued	Low Xmit NowBytesQueued is the current number of bytes in the retransmit queue for low priority traffic.
N	Low Xmit MaxBytesQueued	Low Xmit MaxBytesQueued is the maximum number of bytes observed in the retransmit queue for low priority traffic.
N	Low TotalQoSReallocations	Low TotalQoSReallocations is the total number of times QoS resources had to be reallocated for low priority connection because usage has exceeded previous allocation over defined threshold levels.

To 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 1and 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.

9 Capacity Planning

The purpose of capacity planning is to:

- **Determine Current Solution Capacity:** "How close to the ceiling am I today?"
- **Estimate Growth Potential:** "With current growth plans, when do I upgrade hardware?"
- **Answer "What If" Scenarios:** "What if I add 200 agents?"

Capacity planning is not a one-time task—it should be part of routine contact center operations. A reliable capacity management plan helps prevent outages because the data supports proactive modifications to the deployment that ultimately prevent a particular outage. How might this happen?

For example:

> When the system was initially designed and deployed, it was sized for a specific number of agents with a certain number of skills groups configured per agent. At that time, there was sufficient room to accommodate modest growth. As time went on, small changes occurred with no hint of an issue in capacity – agents were added, skill groups were added. There was no capacity management plan in place and utilization increased with no one being aware. Eventually, utilization was near maximum thresholds where in the midst of a busy period, an unexpected outage occured. If a capacity management plan was in place, the increase in utilization would have been seen with each change to the system. As utilization increased nearing maximum capacity, either additional changes would have been curtailed or an upgrade of hardware would have been done to accommodate the additional changes, thus preventing an outage.

Platform (server hardware) resource utilization data is at the foundation of capacity analysis. The health monitoring performance counters discussed in the prior section are used to determine the capacity utilization of the server. This section describes the process recommended and the reasons for doing routine capacity analysis and planning.

Capacity Planning Requires the Following Action Steps:

1. Collect Data:
   - Initiate data sampling
   - Collect samples after a defined monitoring period
2. Categorize Data:
   The collected data is distributed into three buckets that equate to three different levels:
   a. Hardware Level: resources on a single server
   b. Component Level: resources associated with a single application or a single application component (for example, Unified ICM/Unified CCE Router) on a multi-application or multi-component server
   c. Solution Level: collective utilization level across the entire solution
3. Analyze Data for Target Categories

Use the methods and calculations provided in section *9.4 - Calculating Capacity Utilization* to determine utilization levels for each category.

After the data is collected, categorized, and analyzed, it can then be related to:

1. Today's utilization: A baseline - where am I at today?
2. Recent changes: What effect did the recent change have compared to the baseline?

3. Tomorrow's plans: "What If?" Scenarios: If I add 200 agents, what will likely be the effect?

9.1 Capacity Planning Process

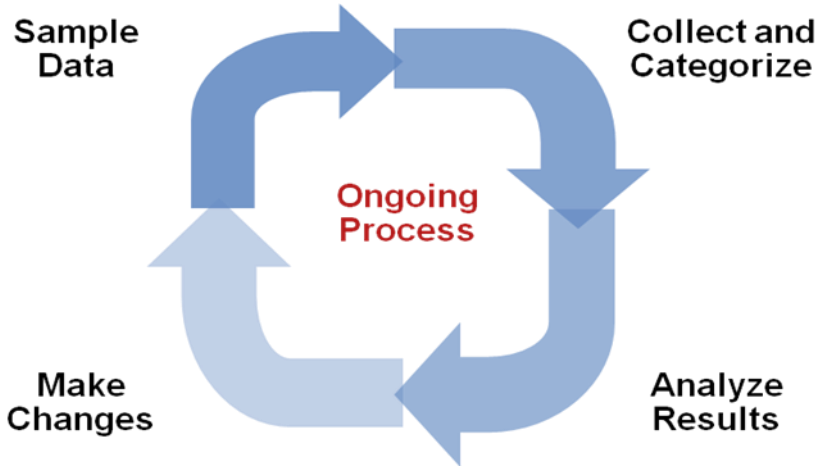


Figure 25: Capacity Planning Process

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

1. **Sample Phase**
   - Initiate 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 exactly the same it was done before you ensure that an equal comparison is made.

9.2 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 – preferably 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.

9.2.1 Finding the "Busy" Hour

To find the busy hour, you must initiate 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 section *9.4 - Calculating Capacity Utilization*. You can set up performance counter values to be written to a disk file in comma separated values (.CSV) format, which is easily imported into a Microsoft Excel workbook. Collect the data sample files, import them into Excel and graph them to see the busy hour. You can import the data set into a graph in a matter of minutes and easily determine the busy hour.

For example:

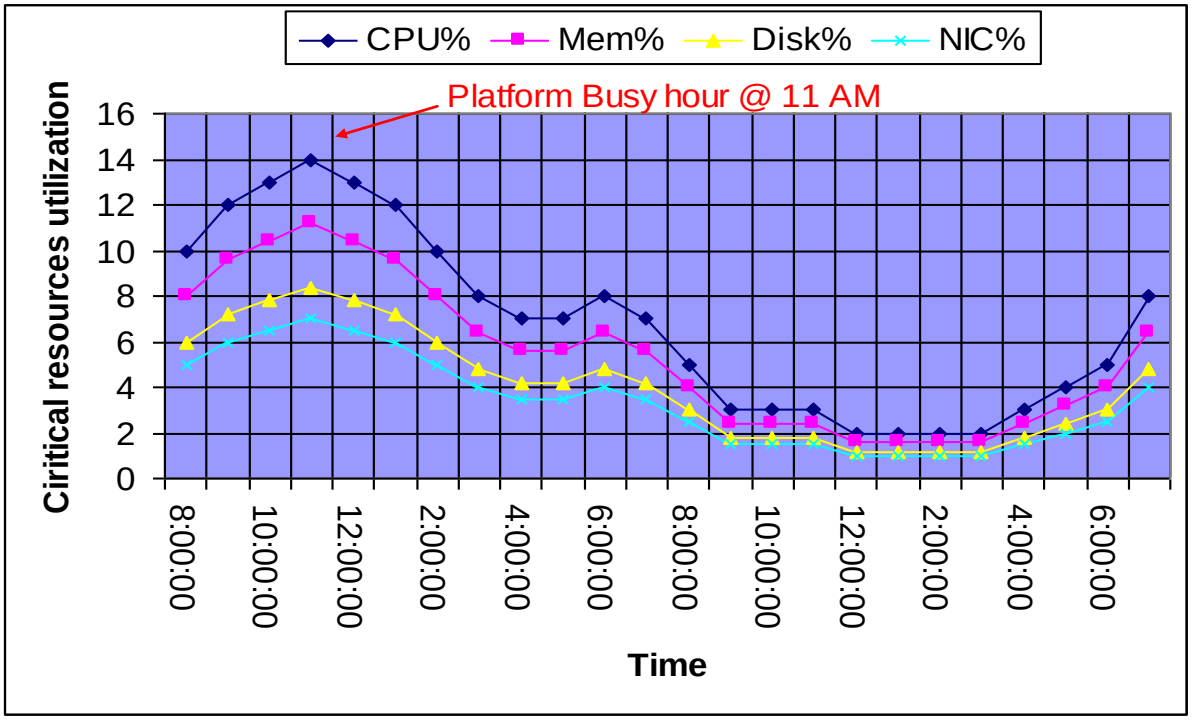


Figure 26: Graph of Samples to Find Busy Hour

9.3 Categorizing Collected Data

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

9.3.1 Current Deployment Design

You must establish and maintain a deployment baseline; this baseline is used to do before/after comparisons. You must establish a new baseline after you make a change in the deployment design.

- Establish an initial baseline – today – with the current deployment design
- Re-establish a baseline after deployment changes occur, such as:
  - Add/delete a Peripheral Gateway
  - Add/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 additional 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, you must maintain deployment information and track changes**:**

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

9.3.2 Configuration Information

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

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

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

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

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

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

Other configuration factors that can affect utilization:

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

9.3.3 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

9.3.4 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 of separations
  - Agents
  - Call Types
  - Reporting
  - Queuing
  - Merging two peripherals into one
- Other requirements
  - Office moving to new location
  - Network infrastructure change: increased/decrease network latency
  - Splitting PG sides over WAN
  - Changing data retention parameters on the HDS

9.3.5 Platform Performance

Any changes in the platform itself can have a corresponding impact on utilization. For example:

- Hardware upgrades
- Software upgrades

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.

9.4 Calculating 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.

The recommended sample rate is one sample every 15 seconds of each of the listed counters. Of the sample set, you can 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. Using this value eliminates short-duration spikes that are statistical outliers.

Counters are divided into two categories:

1. "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.

2. "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 (for more information, see *Hardware and System Software Specification [Bill of Material] for Cisco Unified ICM/Contact Center Enterprise & Hosted* or the *Cisco Unified Contact Center Enterprise Solution Reference Network Design [SRND]*). 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.

9.4.1 Calculating CPU Utilization

Table 9-1: Calculating CPU Utilization

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

9.4.2 Calculating Memory Utilization

Table 9-2: Calculating Memory Utilization

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

9.4.3 Calculating Disk Utilization

Table 9-3: Calculating Disk Utilization

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

9.4.4 Calculating NIC Utilization

Table 9-4: Calculating NIC Utilization

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

9.4.5 Calculating Maximum Utilization

The highest utilization can be determined with:

$$\overline{UTIL_{\rho}} = MAX(\overline{CPU_{\rho}}[t], \overline{Mem_{\rho}}[t], \overline{Disk_{\rho}}[t], \overline{NIC_{\rho}}[t])$$

9.4.6 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.

10 Unified ICM/Unified CCE Diagnostic Tools

The following sections provide information about the configuration, security, and usage, of the Diagnostic Framework.

10.1 Diagnostic Framework

10.1.1 Overview

Beginning with Release 8.0, Unified ICM/Unified CCE/Unified CCH servers have implemented a new web-based service called the Diagnostic Framework, which is used 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 the Diagnostic Framework API section, 10.3.

You can use the Diagnostic Framework as follows:

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

For more information about how to access the service, see section *10.1.4 Usage*.

10.1.2 Installation and Configuration

The Diagnostic Framework service is installed as part of the Unified ICM/Unified CCE/Unified CCH Release 8.0 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.

10.1.2.1 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[1]. 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

[1] The Unified ICM installer detects and installs the appropriate .NET version.

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 utilizes the Windows HTTP SSL service to provide secure communications between the server and the client. Therefore, you must 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 the Diagnostic Framework service is started.

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, you must start IIS.

10.1.2.2 Service Port Configuration

The Diagnostic Framework listens on TCP port 7890.

If needed, you can change the port number. To change the port number you must update the Diagnostic Framework service configuration file and the certificate registration with Windows. You must change the port number on the CLI and Analysis Manager clients too. Additionally, you must 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 absolutely necessary. To change the TCP port, follow these steps:

1. Stop the Diagnostic Framework service through the Windows service control.

2. Open a command prompt and change the directory to:
   <ICM_Drive>:\icm\serviceability\diagnostics\bin

3. Run the following command and confirm from the output that the certificate binding with the current port is valid:
   DiagFwCertMgr /task:ValidateCertBinding

   For more information about the DiagFwCertMgr utility, see section *10.1.3.3 Certificat Management*.

4. Record the thumbprint of the 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 above command or from the following registry value:
   HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\Serviceability\DiagnosticFramework\CertUsedByDiagFwSvc

5. In the same command window, run the following command to remove the certificate binding from the current port:
   DiagFwCertMgr /task:UnbindCert

6. Launch Notepad and open the service configuration 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.

7. Under Services section, locate the following statement and modify the port number printed after *localhost:* from 7890 to your desired number:
   <add baseAddress="https://localhost:**7890**/icm-dp/rest/AnalysisManager" />

Do not modify the syntax of the URL.

8. Save the file and quit Notepad.

9. Open a command prompt and change the directory to:
<ICM_Drive>:\icm\serviceability\diagnostics\bin

10. Run the following command to bind the certificate to the new port number:
DiagFwCertMgr/task:BindCertFromStore/certhash:<hash of the certificate noted above>
The utility reads the port number from the service configuration file.

11. Read the output and confirm that the above command completed successfully. Optionally, run the DiagFwCertMgr/task:ValidateCertBinding command again to verify the changes to the port number binding.

12. Restart the Diagnostic Framework service.

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

10.1.2.3 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 the section, *10.1.3.3, Certificate Management.*

10.1.2.4 Diagnostic Framework Log Files and Logging Level

The Diagnostic Framework log files are created in the following folder:

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

The Diagnostic Framework uses the industry-standard log4net library to create and manage its log files. There is a configuration file that 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 is 'INFO', and it should be sufficient for most cases. Do not change the logging level unless directed by the TAC.

You can change the log level by editing the following 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>
```

10.1.2.5 Diagnostic Framework Service Resources Requirements

10.1.2.5.1 Reduced Priority

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

10.1.2.5.2 Changing Service CPU Threshold

Some CPU-intensive APIs of the Diagnostic Framework first check the overall system CPU utilization value (%CPU), and 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 10-1: CPU Threshold

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

10.1.2.5.3 Changing 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, due to special circumstances if you must lower the number of concurrent requests, then you can modify the value of maxConcurrentCalls property in the service configuration file.

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 following property and change the value to any number below 20:
   <serviceThrottling maxConcurrentCalls="20" />

4. Save the file and quit Notepad.

5. Restart the Diagnostic Framework service.

Caution: Do not increase the value beyond 20. It may lead to unexpected results during peak call volume.

10.1.3 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.

10.1.3.1 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:

1. *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.
2. *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:
   a. Stop the Diagnostic Framework service.

   b. 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.

   c. Locate the following property and change the value from 1 to 0:
      <add key="DomainAuthorizationEnabled" value="1" />

d. Save the file and quit Notepad.

e. 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 follow best practices and set strong password policies. For more information about system hardening and password policies, see the Security Best Practices Guide for Unified ICM/Unified CCE/Unified CCH Release 8.0.

10.1.3.1.1 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 table below summarizes the all authorization combinations. Remember that you can completely disable domain authorization through the service configuration file.

Table 10-2: Domain Authorization Combination

Unified ICM Instances on Server	User Type	Instance Name Provided	Authorization Criteria	Response Content on Successful Authorization
Multiple	Domain	No	Fail authorization, user must	HTTP 403 – Access

Unified ICM Instances on Server	User Type	Instance Name Provided	Authorization Criteria	Response Content on Successful Authorization
			provide instance name in request	Forbidden
Multiple	Domain	Yes	Authorize against the instance name provided by user	Data for instance requested
Multiple	Local	No	Authorize against local group	Data for all instances
Multiple	Local	Yes	Authorize against local group	Data for instance requested
Single	Domain	No	Automatically detect the instance name and authorize against it	Data for instance installed
Single	Domain	Yes	Authorize against the instance name provided by user. If the instance name is invalid then authorization fails.	Data for instance installed
Single	Local	No	Authorize against local group	Data for instance installed
Single	Local	Yes	Authorize against local group	Data for instance installed

10.1.3.2 Encryption

Diagnostic Framework uses SSL to secure the HTTP connection between the server and the client. This secures both the credentials as well as data exchanged. To establish the SSL connection, a self-signed certificate is created by the ICM-CCE-CCH installer and used 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.

10.1.3.3 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 then Cisco recommends that you replace the self-signed certificate with a trusted third-party certificate to provide improved security[2].

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.

10.1.3.3.1 Diagnostic Framework Certificate Manager Utility

The Diagnostic Framework Certificate Manager utility is a command line utility used to manage certificate creation and binding for the Diagnostic Framework service. It is installed at:

<ICM_Drive>:\icm\serviceability\diagnostics\bin\DiagFwCertMgr.exe

The utility can perform the following tasks:

- Create self-signed certificate.
- Store the certificate in Local Computer Personal certificate store.
- Bind a certificate to Windows HTTP service on a given port.
- Remove a certificate binding from the Windows HTTP service on a given port.
- Delete the self-signed certificate created by itself from the Local Computer Personal certificate store.
- Validate the certificate binding to HTTP service for Diagnostic Framework service.

The following section explains the usage of the utility:

DiagFwCertMgr /task:<task_name>

[/port:<port_number>]

[/certhash:<certificate_thumbprint>]

[/logpath:<logfile_path>]

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.

[2] 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.

/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 10-3: Diagnostic Framework Certificate Manager Utility Tasks

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

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.

10.1.3.3.2 Using a Trusted Third-party Certificate

Replacing the certificate used by the Diagnostic Framework service involves two tasks, first to **import** the new certificate in the Local Computer Personal certificate store and second 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 as explained in 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

Note: To import a certificate in the Local Computer Personal certificate store in Windows 2008, follow the same instructions.

Caution: Do not follow the instructions in the next section "*Assign the Imported Certificate to the Web Site*." Diagnostic Framework does not use IIS web server. It is hosted on top of Windows HTTP service. You must use the DiagFwCertMgr utility to bind this certificate to the Windows HTTP service.

Bind Certificate: Follow the instructions below 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 that needs to be used 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 following command to remove the current certificate binding from the port:
   DiagFwCertMgr /task:UnbindCert

5. Run the following command to bind the new certificate to the service:
   DiagFwCertMgr /task:BindCertFromStore /certhash:<hash of the certificate noted above>
   The utility reads the port number from the service configuration file.

6. Read the output and confirm that the above command completed successfully. Optionally, run the DiagFwCertMgr /task:ValidateCertBinding command to verify the changes to the certificate binding.

7. Restart the Diagnostic Framework service.

10.1.4 Usage

The framework provides four ways to access the diagnostic data:

10.1.4.1 Accessing the Diagnostic Framework through the Analysis Manager

The Analysis Manager is part of the Real Time Monitoring client Tool (RTMT) that resides on Unified CM. RTMT is not a web-based tool, rather it is a thick client tool that you must download from the Unified CM and install on a server. RTMT includes menus for the

Analysis Manager. You can access the Analysis Manager functions from the tool. See the sample screen:

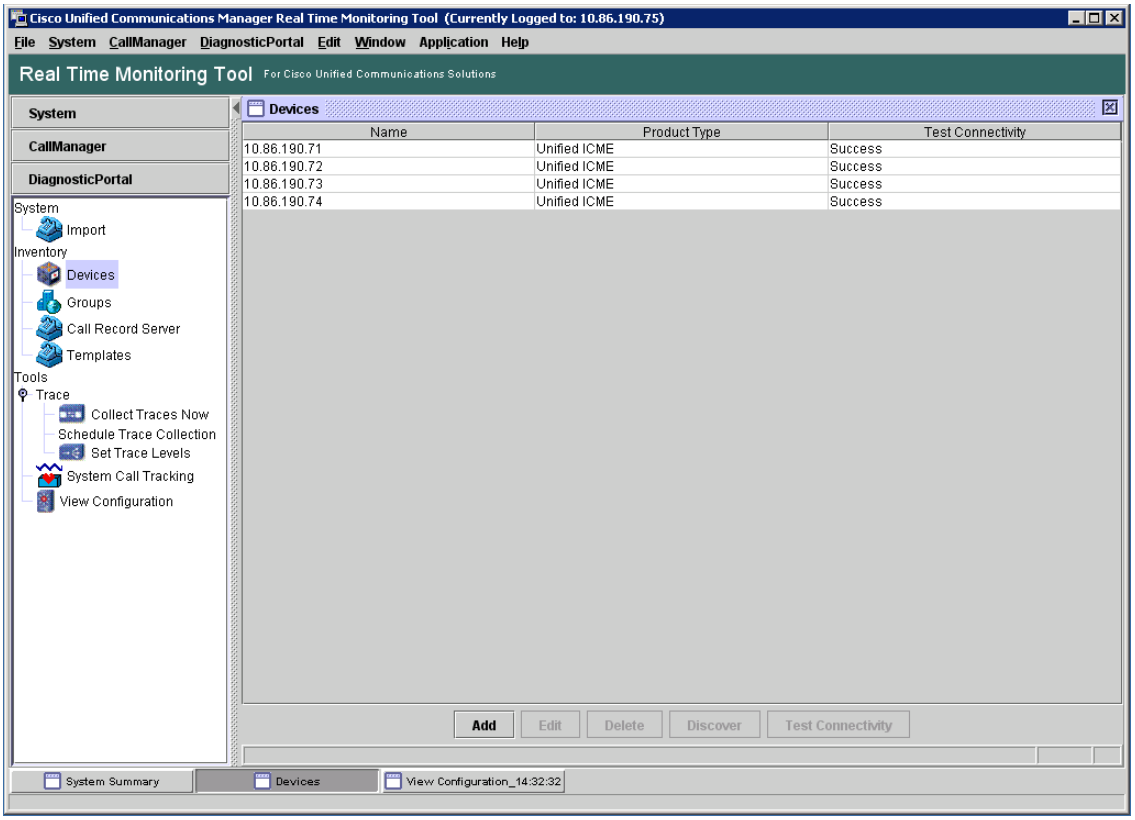


Figure 27: Real Time Monitoring Tool

For more information about how to use the Analysis Manager, see the *Cisco Real-time Monitoring Tool Administration Guide*.

10.1.4.2 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 the following location:

<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).

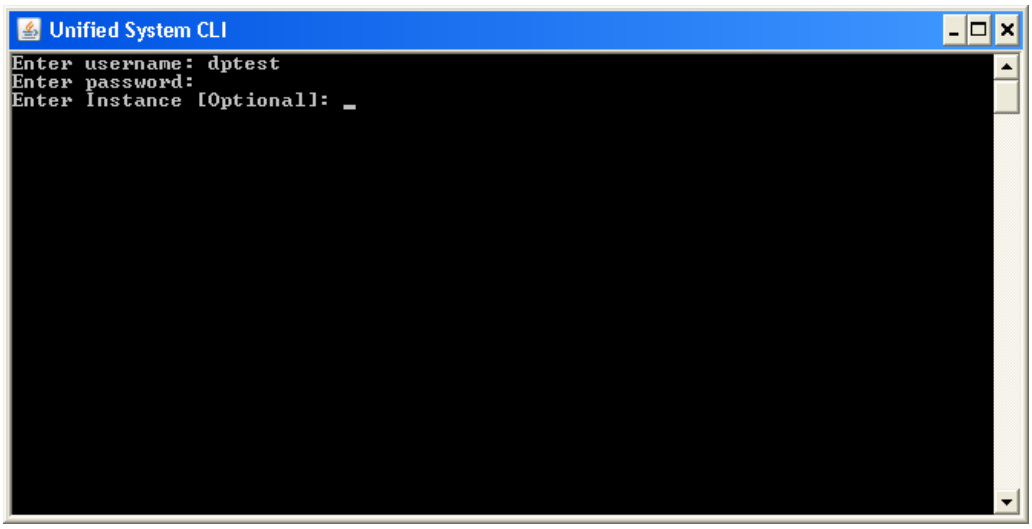


Figure 28: Using Unified System CLI from Command Prompt

On authentication, you can use the CLI from this window, as explained in the following section.

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. Fore more information, see the section *Special Consideration for Servers with Multiple ICM Instances*.

10.1.4.2.1 Unified CLI Architecture

Note: This figure is only from a Unified CVP perspective, and does not directly specify the Diagnostic Framework. However, the Diagnostic Framework is what the Unified CCE uses as an underlying implementation.

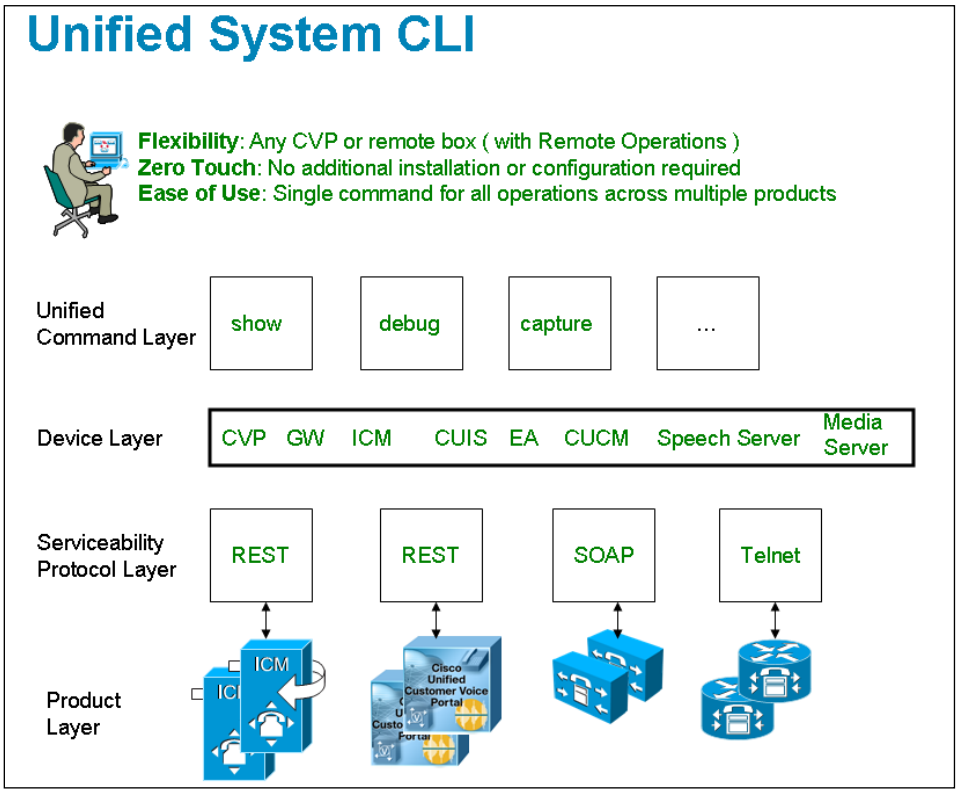


Figure 29: Unified CLI Architecture

A user can perform the following tasks using the Unified CLI:

- Run a single command (in system mode) on any Unified CCE system to gather information about all supported solution components.
- In system mode, you can optionally provide the seed devices in WSC_CLI_DIR\conf directory or give a flat CSV file with a device list.
- System mode allows the CLI to recursively go to each supported box in the background and run the same command that was executed by the user 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.
- The system command can also be executed 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.

10.1.4.2.2 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.

10.1.4.2.3 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.

10.1.4.2.4 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:

Notes:

1. If you do not specify component/sub-component, then the list includes all the installed components/sub-components on the server.
2. The command output on screen does not include binary data.

Table 10-4: CLI Commands

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

Notes:

- 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. For your convenience this information is posted below.

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.

Table 10-5: Syntax and Examples

Noun	Parameters and Options
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". 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. 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 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 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). **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 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. **The following is the list of 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:** show license [options] This command displays the license data. **Options:** 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). **Example:** show license **In system mode,** show license devicetype ios|cvp|ucm show license server 10.86.129.123(ucm) show license group GroupB|default To save the output to a directory, show license redirect dir c:\temp\ -- the output is saved in c:\temp\clioutput.zip. To save the output to a text file, show license redirect file c:\temp\output.txt
show log	**Syntax:** show log [options] Displays contents or downloads (if redirect option is used) the product *miscellaneous* log file(s) for a component or subcomponent. **Options:** component - narrow the output to the specified component(s). subcomponent - narrow the output to the specified subcomponent(s). absdatetime - narrow the output to the specified time range in the form of start time and end time.Time format is "mm-dd-yyyy:hh:mm". reltime - narrow the output to the specified time range in the form of relative time from the current time. match - narrow the output to the specified regex pattern. This match pattern is applied to text based log output only. redirect - redirect the output to a file or a directory. **Additional system 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).

	Example: show log component cvp:callserver - displays contents of all the log files for component cvp:callserver; can be a huge output show log component cvp:vxmlserver absdatetime 9-18-2008:14:00 9-20-2008:18:00 - displays contents of all the log files for component cvp:vxmlserver based on specific start date,time and end date, time values show log component cvp:vxmlserver absdatetime 9-18-2008:14:00 13:00 - displays contents of all the log files for component cvp:vxmlserver based on specific start date,time and end time values. show log component cvp:callserver subcomponent sip reltime 10 minutes – displays contents of all the log files based on elapsed time of 10 minutes for component cvp:callserver and subcomponent cvp:sip show log component cvp:callserver absdatetime 9-18-2008:14:00 13:00 match .*CVPS ervlet.* - displays contents of all the log files based on match criteria, time range for component cvp:callserver show log component cvp:callserver absdatetime 9-18-2008:14:00 13:00 match .*CVPServlet.* redirect file c:\uccelogs - downloads all the log files on match criteria, time range for component cvp:callserver To save the output to a directory, show log redirect dir c:\temp\ -- the output is saved in c:\temp\clioutput.zip. To save the output to a text file, show log redirect file c:\temp\output.txt
show perf	**Syntax:** show perf [options] This command displays performance data. **Options:** component - narrow the output to the specified component(s). subcomponent - narrow the output to the specified subcomponent(s). redirect - redirect the output to a file or a directory. **Additional system 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. **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 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). **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 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). **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 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. **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 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). **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 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). **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 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. **Each product translates following levels to product specific debug level setting** . - 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 dtcomponent "ucm:Cisco CallManager|cup:Cisco UP SIP Proxy|cvp:CallServer" To save the output to a specific 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

Note: The filter and match features of the CLI are not supported for trace files because the framework returns a zip file that contains not just the text file. For those two features, CLI expects a plain text file.

Following is the system mode syntax:

Note: You can add product specific extensions; however**.** any extension must be reviewed by this common cross-product team for clarity and consistency.

Table 10-6: System Mode Syntax

Command (Verb)	Noun	Description
system		Enter the interactive system mode of the CLI. Use quit/exit command to exit the system mode.

The system command can also be executed by prefixing the "system" on any regular command for non-interactive mode. For example, "system show all".

Table 10-7: System Commands

Noun	Parameters and Options	Description
show all	[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 **blue** color above are included to commands in system mode. where **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.	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

Noun	Parameters and Options	Description
	 Warning Because running this command can affect system performance, Cisco recommends that you run the command during off-peak hours.	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 "10.86.129*" 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

Noun	Parameters and Options	Description
		Output is saved to "c:\system-tech-support\clioutput0.zip" Example-5: admin:**system show all redirect ftp://vpalawat:password/SR609140000** [server-1] server-1 show all Output [server-2] server-2 show all Output [server-3] server-3 show all Output [server-4] server-4 show all Output [server-5] server-5 show all Output [server-6] server-6 show all Output Output is saved to "ftp-sj.cisco.com\incoming\SR609140000-0.zip" Output is saved to "ftp-sj.cisco.com\incoming\SR609140000-1.zip" Example-6: Assuming that devices configured in OAMP are CVP[server-5], IOS [server-2, server-3], UCM [server-4] and ICM [server-1] . admin:system admin(system):**show all devicetype cvp|ios redirect dir c:\system-tech-support** [server-2] server-2 show all Output of ProductType [ios] [server-3] server-3 show all Output of ProductType [ios] [server-5]

Noun	Parameters and Options	Description
		server-5 show all Output of ProductType [cvp] Output is saved to "c:\system-tech-support\clioutput0.zip"

10.1.4.2.5 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, Cisco recommends that you run the command during off-peak hours.

10.1.4.2.6 Import File Syntax

The file to be imported is named devices.csv in:

<ICM_Drive>:\icm\serviceability\wsccli\conf

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.

10.1.4.2.6.1 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 Intellegence Center
#    * CUP        - For Unified Presence ( that includes the SIP Proxy )
################################################################################
#
# The column assignments are as follows:
#
# HOSTNAME                -- Mandatory
# DESCRIPTION
# PRODUCT_TYPE            -- Mandatory
# GROUP
# USERNAME
# PASSWORD
# PORT_NUMBER             -- Mandatory
# ENABLE_PASSWORD
# IS_SEED_SERVER
#
HOSTNAME, DESCRIPTION, PRODUCT_TYPE, GROUP, USERNAME, PASSWORD,
PORT_NUMBER, ENABLE_PASSWORD, IS_SEED_SERVER
#10.86.129.109, IOS GW, IOS, Location_1, cisco, cisco, 23, cisco,,
```

Note: All references to ICM in the above text file equal Unified CCE.

10.1.4.2.7 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 10-8: Device, Protocol and Command Mapping

	CVP	Unified CCE	EA	CUIC	Speech Server	Media Server	Trace Server	IOS GW	Unified CM	Unified CCX
capture	REST				REST	REST	REST			
config	REST	REST	REST	REST				TELNET		
debug	REST	REST	REST	REST				TELNET	SOAP	REST
license	REST	REST	REST	REST				TELNET	SOAP	REST
log	REST	REST			REST	REST	REST			
perf	REST	REST			REST	REST	REST	TELNET		
platform	REST	REST	SOAP	SOAP	REST	REST	REST	TELNET	SOAP	SOAP
sessions	REST							TELNET		

trace	REST	REST	SOAP REST	SOAP REST	?	?	?	TELNET	SOAP	SOAP REST
version	REST	REST	SOAP REST	SOAP REST	REST	REST	REST	TELNET	SOAP	SOAP REST

-- 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.

10.1.4.2.8 Mapping of System CLI commands to IOS CLI commands

Table 10-9: Mapping of System CLI commands to IOS CLI commands

System CLI	IOS CLI	Notes
"show config"	"show running-config"	
"show version"	"show version"	
"show license"	"show license"	
"show perf"	"show call resource voice stat" "show memory statistics" "show processes cpu history" "show processes memory sorted" "show voice dsp group all" "show voice dsp voice"	
"show debug"	"show debug"	
"show log"	N/A	
"show sessions"	"show call active voice compact"	
"show tech-support"	"show tech-support" <Everything else given above>	
"show trace"	"show logging"	

"show platform"	"show diag"	
"debug"	0 no debug all 1 - deb ccsip err deb cch323 err deb voip app vxml err deb http client err deb mrcp err deb rtsp err deb h225 asn1 err deb h245 asn1 err 2 - debug isdn q931 debug h225 events debug h245 events debug voip ccapi inout debug vtsp events 3 - debug ccsip messages debug h225 q931 debug h225 asn1 debug h245 asn1	

Note: This mapping table is available in the configuration file, so that mapping can be easily altered.

10.1.4.2.9 Logs

You can find all logs generated by the CLI process under the following directory:

<ICM_Drive>:\icm\serviceability\wsccli

10.1.4.3 Accessing the Diagnostic Framework via 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 browser. 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:

https://<UCCE-server>:<port>/icm-dp/rest/DiagnosticPortal/GetMenu

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.

Note: 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:

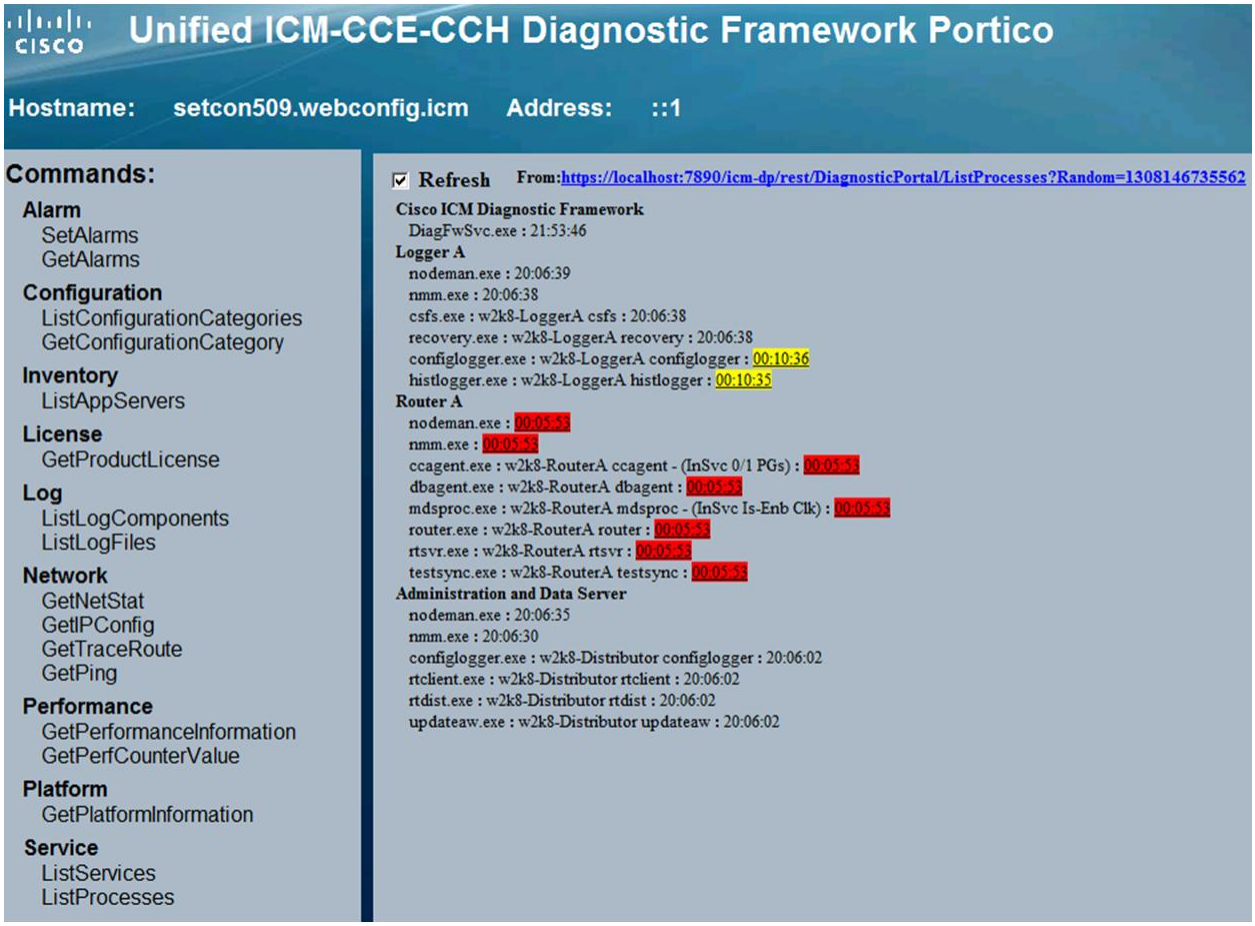


Figure 30: Unified ICM-CCE-CCH Diagnostic Framework Portico

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.

- When a process restarted (more than 10 minutes ago but less than 30 minutes ago) uptime is yellow.
- When the status of a process as defined inside the parentheses changes, the process is bolded and highlighted in blue for 10 minutes or until it returns to its former state.

191

parameters; it generates another zip file with exactly the same contents but with a different file name.

10.1.4.4 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:

https://<UCCE-Server>:<port>/icm-dp/rest/AnalysisManager/GetTraceLevel?Component=Component/Subcomponent

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 the API section.

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

Note: 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** in **Security** option (Path: **Tools**>**Internet Options > Advanced Tab**) is unchecked.

10.2 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, which is the preferred method for the following reasons:

1) All devices are centrally added to and stored in CVP OAMP. One update on OAMP will be reflected in all CLI clients.
2) Passwords for devices are encrypted in OAMP.
3) CVP Remote Operations can be installed on any Windows machine, such as a personal laptop, simplifying setup and access to all devices.

Customers without CVP OAMP can still utilize the CLI using a CSV file for connection information. See "Deployment Option 2: Devices.csv".

10.2.1 Deployment Option 1: CVP OAMP

10.2.1.1 System CLI Configuration with CVP OAMP

The first step for setting up System mode is to add all of the devices in your deployment to CVP OAMP.

1. Sign in to CVP Operations Console from a web browser and navigate to **Device Management > Unified ICM**.

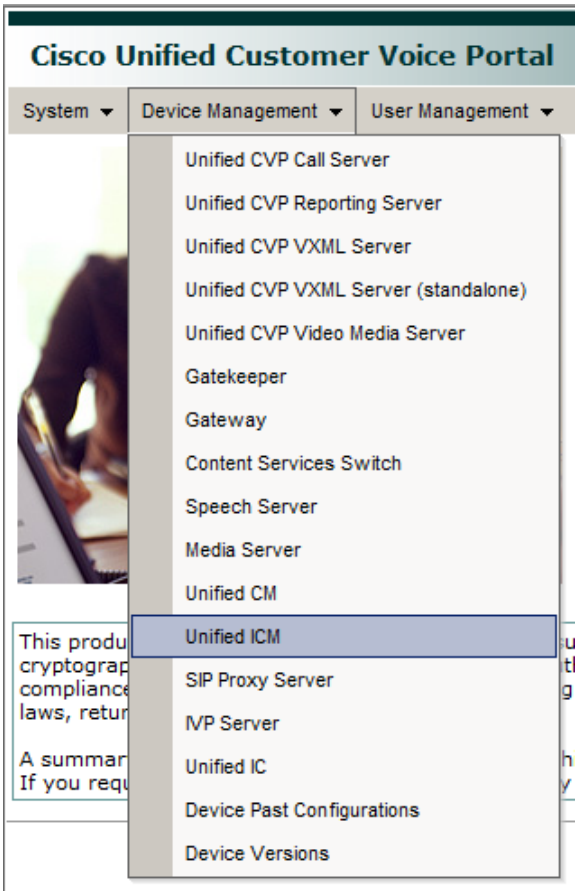


Figure 31: CVP Operations Console

2. Click **Add New** and populate the IP Address, Hostname, and Description fields.

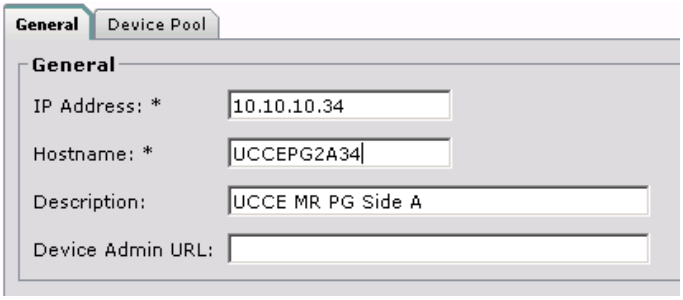


Figure 32: IP Address, Hostname, and Description fields

3. Check **Enable Serviceability**. Populate the Username and Password fields with sign-in credentials for that particular device. Leave the default port as 7890.

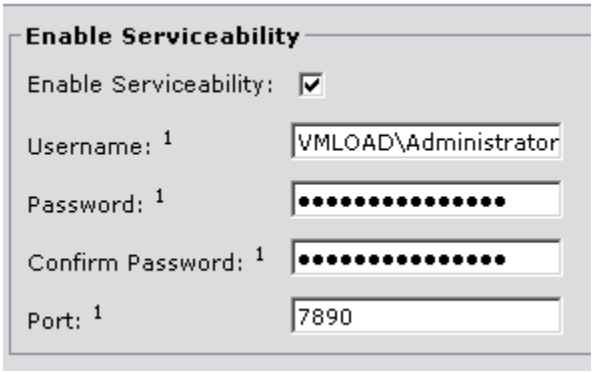


Figure 33: Username, Password and Port fields

4. Click the **Device Pool** tab and associate the device with a group if desired. (Tip: Create a "UCCE-SideA" group for all devices on the A-side.)

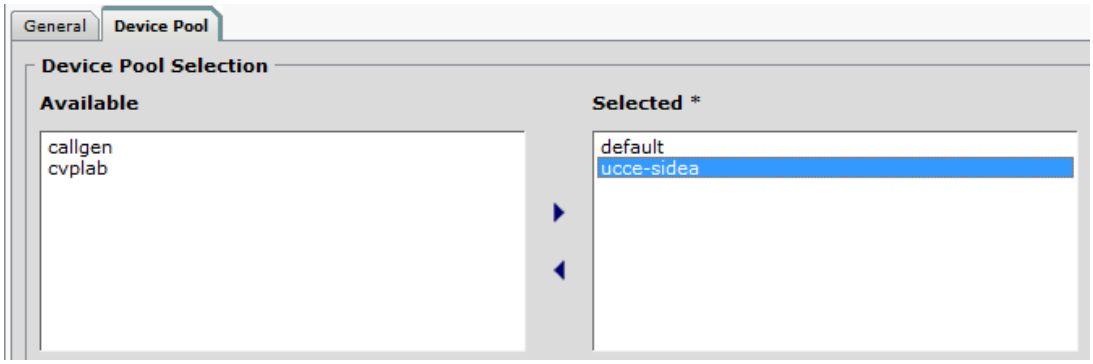


Figure 34: Device Pool Selection

5. Click **Save**.

Repeat the above process for all other devices: UCCE, CUIC, UCM, Gateways, and so on.

10.2.1.2 Confirm or Add a User to CVP OAMP for the 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:

1. In the CVP Operations Console, click **User Management > Users**.
2. To modify an existing user, click **wsmadmin** in the List of Users.
3. To add a new user, click **Add New**.
4. Once the new username and/or password have been entered, click the **User Groups** tab and add the "ServiceabilityAdministrationUserGroup" to the "Selected" bucket on the right side.
5. Click **Save** to complete any updates or additions.

10.2.1.3 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.

1. Run the CVP 8.5 Installer and select the Remote Operations checkbox.

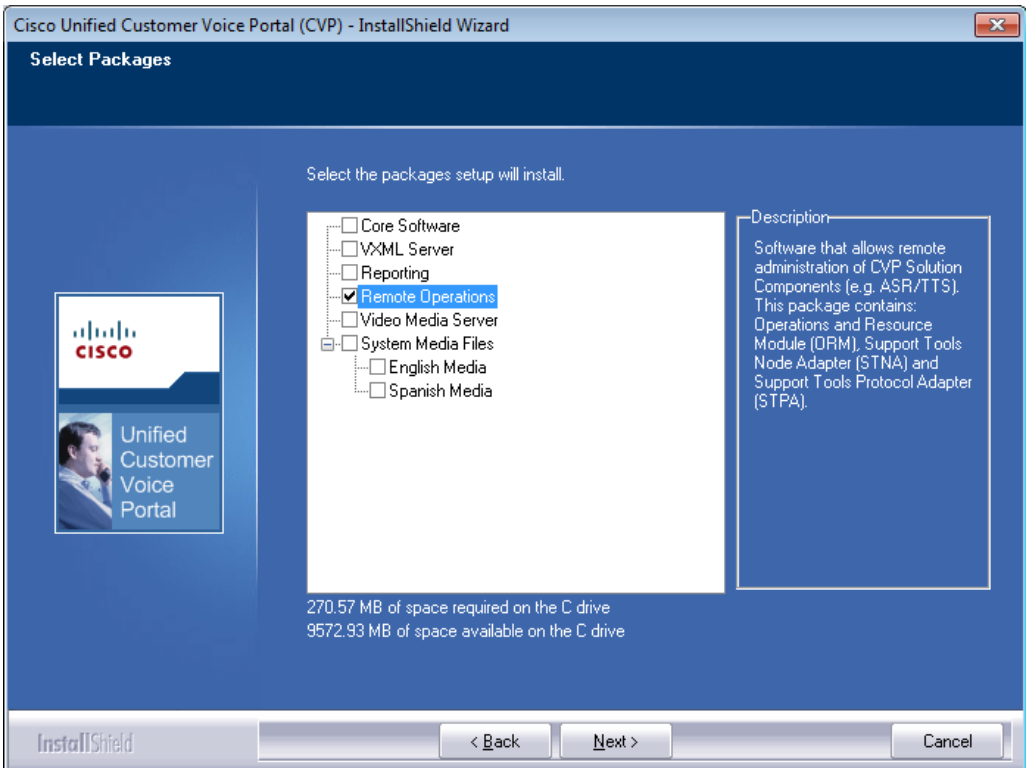


Figure 35: Remote Operations installation

2. If installing on Windows 7, ignore the "Unsupported OS" warning and click **OK**.

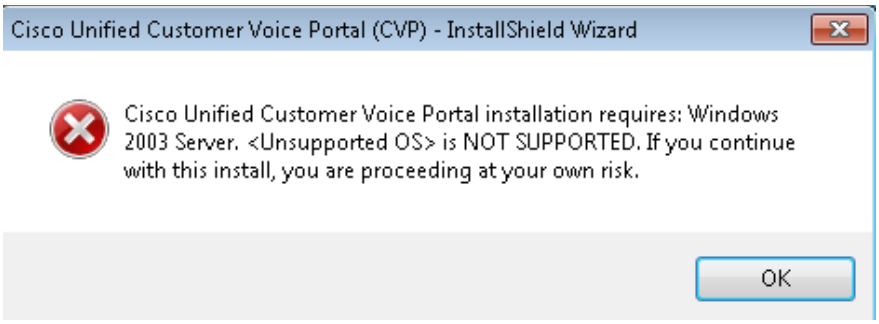


Figure 36: <Unsupported OS> error message

3. Apply security hardening if desired, then complete installation.

10.2.1.4 Add Remote Operations Machines to CVP Operations Console

1. Open a web browser and sign in to the CVP Operations Console. Navigate to **System > Web Services**.
2. Click the **Remote Operations Deployment** tab on the subsequent screen.
3. Enter the IP address and hostname of the machine where CVP Remote Operations was just installed. Include a description if desired and click **Add**.

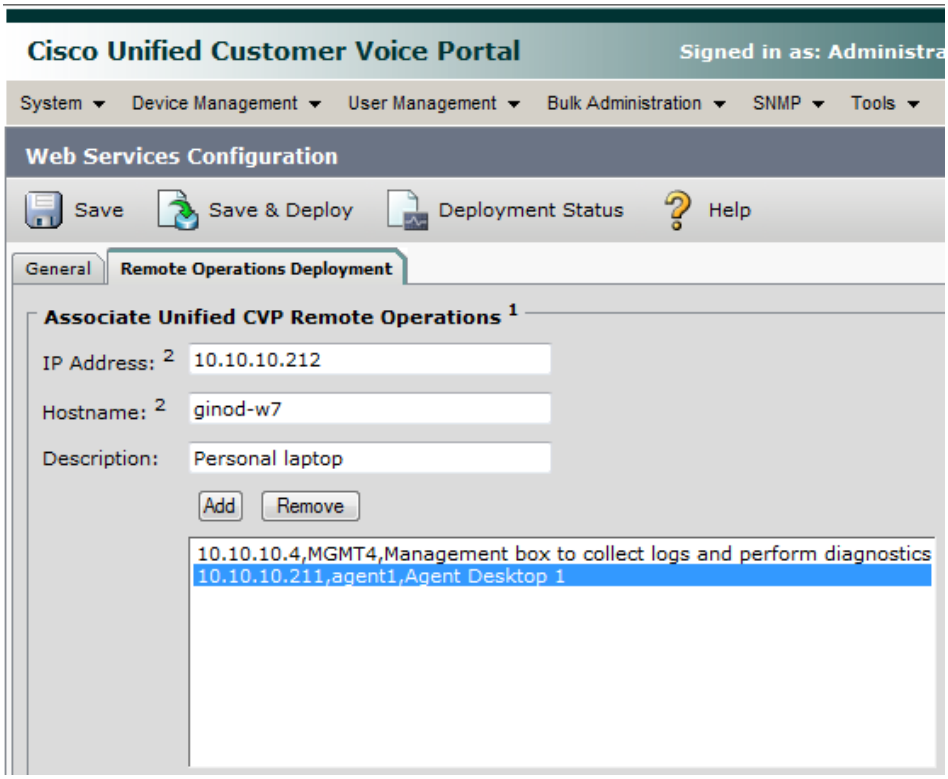


Figure 37: Web Services Configuration

4. Repeat for any additional Remote Operations machines, then click **Save & Deploy** to make this device available for Remote Operations.
5. You will be informed that the Web Services configuration deployment is in progress. Click the **Deployment Status** button to verify the status of the newly-added machine(s). Click the **Refresh** button until the status changes to "Success".

10.2.1.5 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.

1. On the Remote Operations machine, click **Start > Run** and enter "systempropertiesadvanced".
2. Click **Environment Variables**.
3. Confirm the System Variable WSC_CLI_DIR is set to "C:\Cisco\CVP\wsm\CLI".
4. Confirm the Path variable contains "C:\Cisco\CVP\wsm\CLI;".

10.2.1.6 Start Using the 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.

1. Open the Unified System CLI on the new Remote Operations machine from **Start > Programs > Cisco Unified Customer Voice Portal > Unified System CLI**.

2. Sign in with user wsmadmin (or sign in with the new user).
3. Enter System mode by typing "system". Servers that are successfully discovered are indicated by a '.' while servers not discovered are indicated by "Unable to connect".
   Once initial connection is complete, (system) will be displayed in the command prompt (see below). All commands entered while in System mode will be run against all reachable devices defined in CVP OAMP.

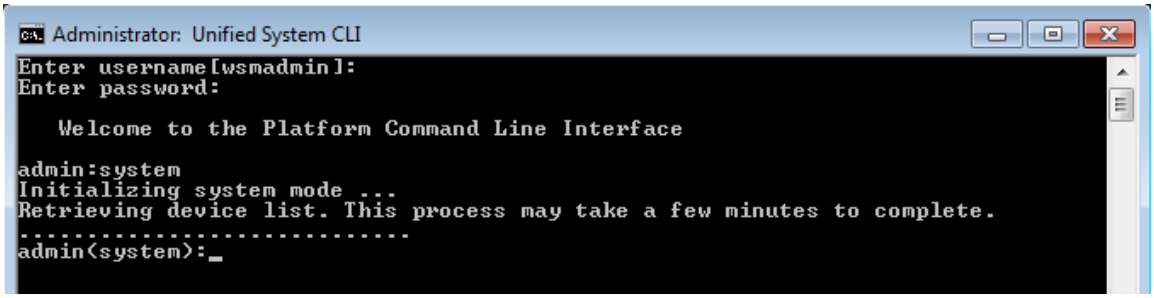


Figure 38: Unified System CLI

Any changes made in OAMP while a CLI session is active will not be reflected immediately. There are two options for receiving the updates:

a. Close the console window and start a new connection.
b. Type "exit" to leave System mode and then "system init"

10.2.2 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.

10.2.2.1 Create Devices.csv from Sample File

1. Navigate to C:\icm\serviceability\wsccli\conf\.
2. Make a copy of devices-sample.csv and save it as devices.csv.

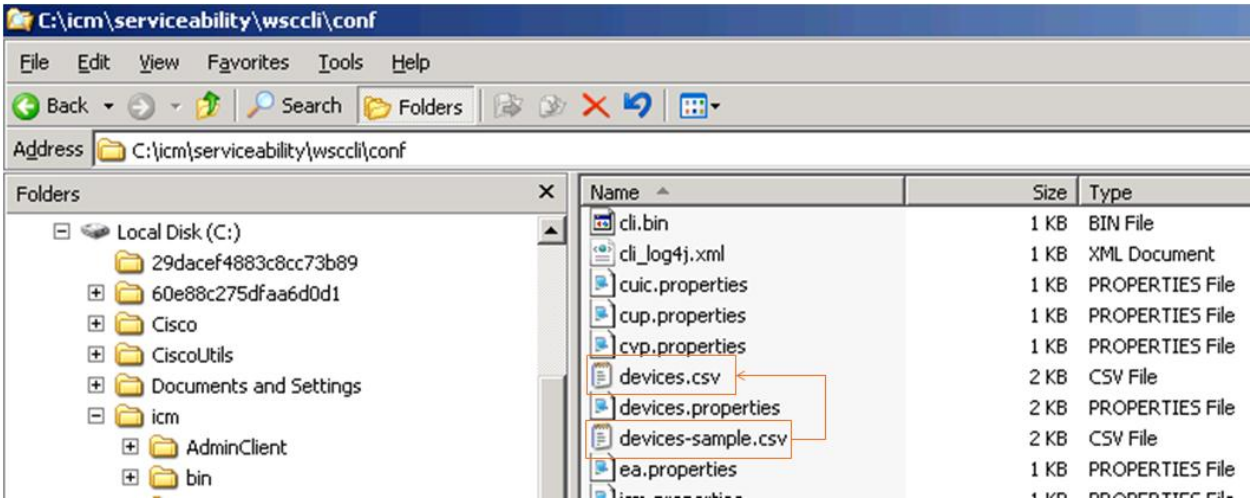


Figure 39: devices-sample.csv

10.2.2.2 Populate New devices.csv with connection information

Each device must be added on its own line at the bottom of the devices.csv file.

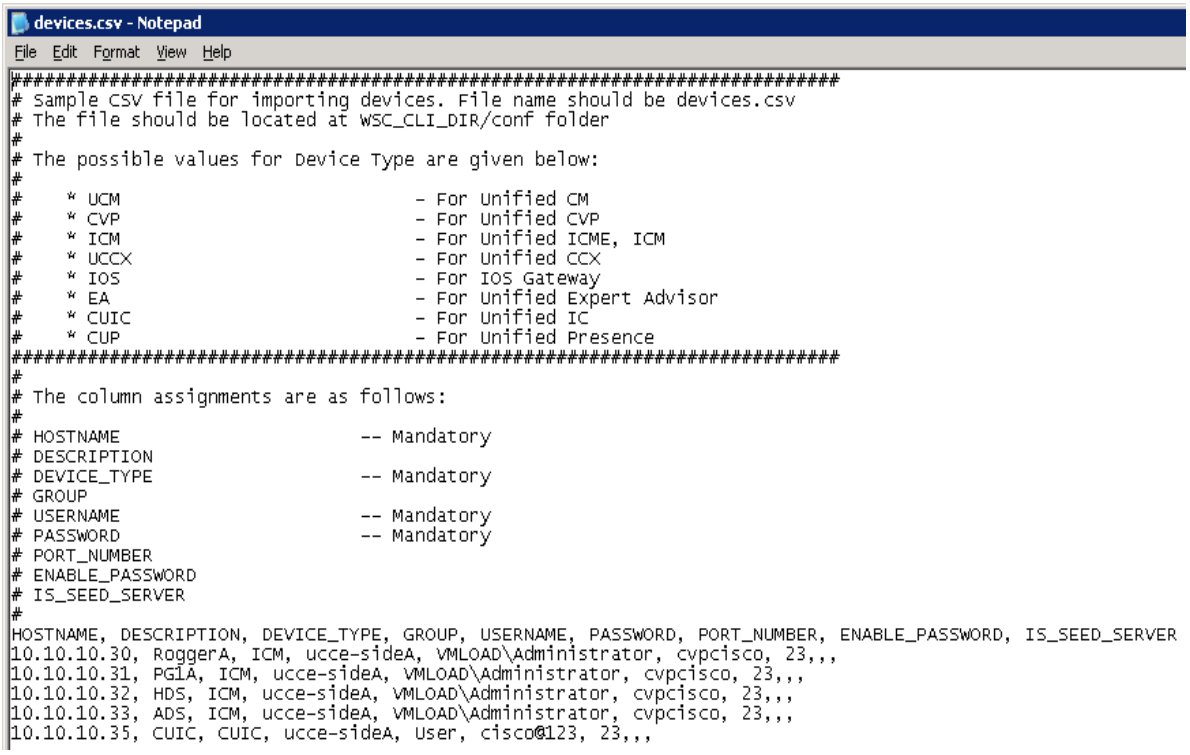
1. Within each line you must specify the following required fields:
    a. IP address and hostname
    b. Device Type (from the options listed at the top of the file)
    c. Username
    d. Password – this is typically the deal-breaker for most customers as it will be stored in plaintext.
    e. Port Number (leave the default 23 in most cases)

In addition, the following fields are recommended to make usage easier:

    a. Description
    b. Group (for example, UCCE-SideA)

2. Save **devices.csv** when complete.

An example of a completed devices.csv.



devices.csv - Notepad

File Edit Format View Help

```
################################################################################
# Sample CSV file for importing devices. File name should be devices.csv
# The file should be located at WSC_CLI_DIR/conf folder
#
# The possible values for Device Type are given below:
#
#    * UCM                          - For Unified CM
#    * CVP                          - For Unified CVP
#    * ICM                          - For Unified ICME, ICM
#    * UCCX                         - For Unified CCX
#    * IOS                          - For IOS Gateway
#    * EA                           - For Unified Expert Advisor
#    * CUIC                         - For Unified IC
#    * CUP                          - For Unified Presence
################################################################################
#
# The column assignments are as follows:
#
# HOSTNAME                      -- Mandatory
# DESCRIPTION
# DEVICE_TYPE                   -- Mandatory
# GROUP
# USERNAME                      -- Mandatory
# PASSWORD                      -- Mandatory
# PORT_NUMBER
# ENABLE_PASSWORD
# IS_SEED_SERVER
#
HOSTNAME, DESCRIPTION, DEVICE_TYPE, GROUP, USERNAME, PASSWORD, PORT_NUMBER, ENABLE_PASSWORD, IS_SEED_SERVER
10.10.10.30, RoggerA, ICM, ucce-sideA, VMLOAD\Administrator, cvpcisco, 23,,,
10.10.10.31, PGiA, ICM, ucce-sideA, VMLOAD\Administrator, cvpcisco, 23,,,
10.10.10.32, HDS, ICM, ucce-sideA, VMLOAD\Administrator, cvpcisco, 23,,,
10.10.10.33, ADS, ICM, ucce-sideA, VMLOAD\Administrator, cvpcisco, 23,,,
10.10.10.35, CUIC, CUIC, ucce-sideA, User, cisco@123, 23,,,
```

Figure 40: Example of devices.csv

10.2.2.3 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. To validate and add users to this group:

1) Click **Start > Run** and enter "lusrmgr.msc".
2) Click the **Groups** folder and double-click "ICMDiagnosticFrameworkUsers".
3) Add necessary users to the group and click **OK**.

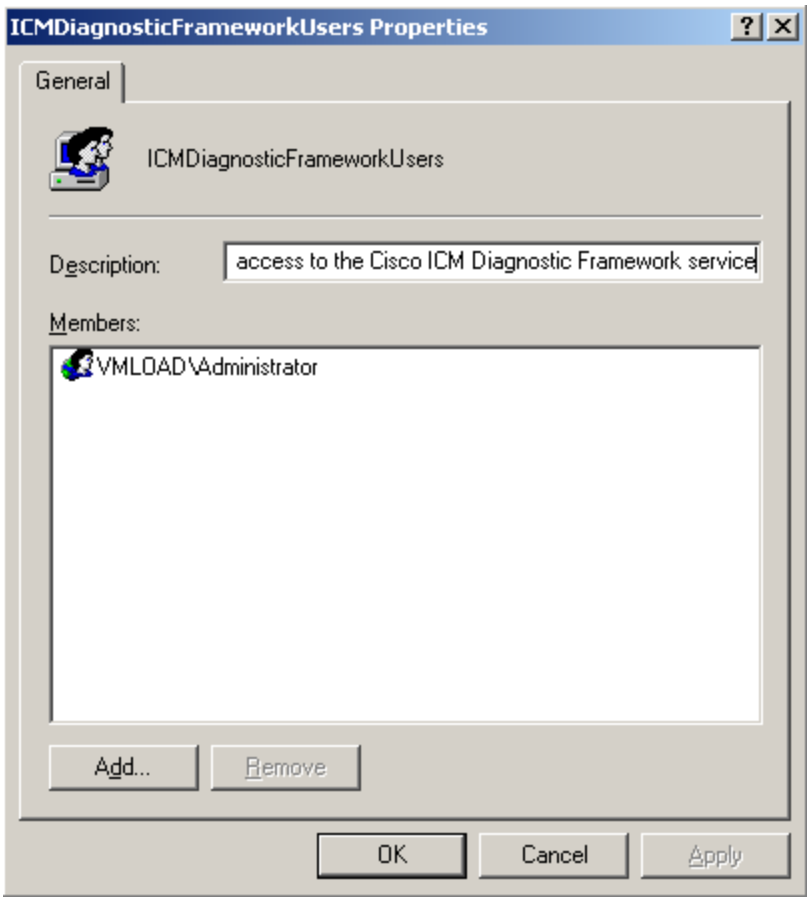


Figure 41: ICMDiagnosticFrameworkUsers Dialog

10.2.2.4 Using the Unified System CLI with Devices.csv

1. On the ADS, click **Start > Programs > Cisco Unified CCE Tools > Unified System CLI**. (If this shortcut is missing for some reason, run C:\icm\serviceability\wsccli\runwsccli.bat).
2. Sign in with a member of the ICMDiagnosticFrameworkUsers group.
3. 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.
4. Once successfully signed in to the 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".
5. Once initial connection is complete, (system) will be displayed in the command prompt (see below). All commands entered while in System mode will be run against all reachable devices defined in devices.csv

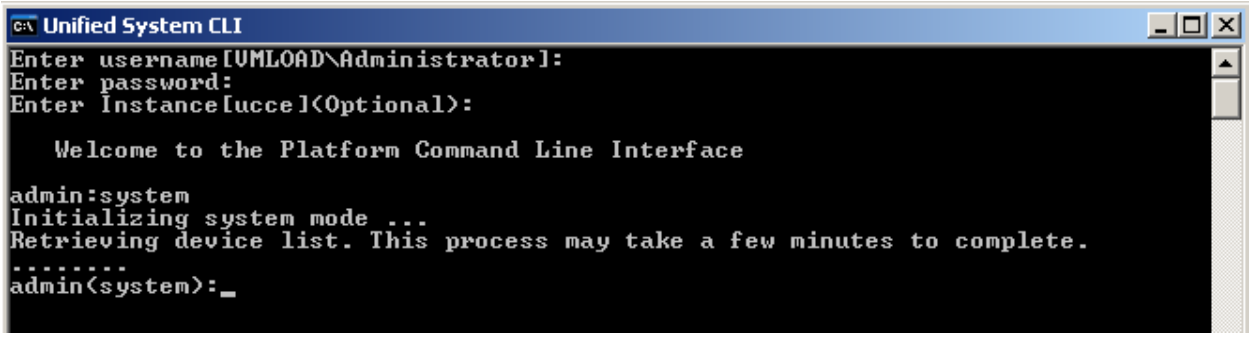


Figure 42: Unified System CLI

10.2.2.5 Running the System CLI from Multiple Machines with Devices.csv

If you intend to run the System CLI on another machine, such as a second ADS, the devices.csv 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.

10.3 Diagnostic Framework API

The Diagnostic Interface supports the following commands.

10.3.1.1 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 10-10: Trace Levels

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

Request:

https://<server>:<port>/icm-dp/rest/AnaysisManager/GetTraceLevel?Component=Component/Subcomponent

Reply example:

```
<?xml version="1.0" encoding="UTF-8"?>
<dp:GetTraceLevelReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/analysismanager">
<dp:Schema Version="1.0"/>
```

```
<dp:Trace Level="0"/>
</dp:GetTraceLevelReply>
```

10.3.1.2 SetTraceLevel

For more information about the trace level values, see GetTraceLevel in the previous section.

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/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/analysismanager">
<dp:Schema Version="1.0"/>
</dp:SetTraceLevelReply>
```

10.3.1.3 ListTraceComponents

Lists all possible application components that produce trace files.

Request:

https://<server>:<port>/icm-dp/rest/ AnalysisManager/ListTraceComponents

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:ListTraceComponentsReply ReturnCode="0" xmlns:dp="http://www.cisco.com/vtg/analysismanager">
<dp:Schema Version="1.0" />
<dp:TraceComponentList>
<dp:TraceComponent Name="Logger A" ComponentType="Logger" Description="ICM Component"
IsLevelConfigurable="true" IsFileCollectable="true">
  <dp:TraceComponentList>
  <dp:TraceComponent Name="baImport" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="CampaignManager" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="clgr" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="csfs" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="cw2kFeed" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="dtp" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="hlgr" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="nm" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="nmm" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="rcv" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="rpl" Description="ICM Process for Component LoggerA"
IsLevelConfigurable="true" IsFileCollectable="true" />
</dp:TraceComponentList>
</dp:TraceComponent>
```

```
<dp:TraceComponent Name="Router A" ComponentType="Router" Description="ICM Component"
IsLevelConfigurable="true" IsFileCollectable="true">
  <dp:TraceComponentList>
  <dp:TraceComponent Name="agi" Description="ICM Process for Component RouterA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="ccag" Description="ICM Process for Component RouterA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="dba" Description="ICM Process for Component RouterA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="dbw" Description="ICM Process for Component RouterA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="mds" Description="ICM Process for Component RouterA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="nm" Description="ICM Process for Component RouterA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="nmm" Description="ICM Process for Component RouterA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="nms" Description="ICM Process for Component RouterA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="rtr" Description="ICM Process for Component RouterA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  <dp:TraceComponent Name="rts" Description="ICM Process for Component RouterA"
IsLevelConfigurable="true" IsFileCollectable="true" />
  </dp:TraceComponentList>
</dp:TraceComponent>
<dp:TraceComponent Name="Cisco ICM Diagnostic Framework" Description="Cisco ICM Diagnostic
Framework" IsLevelConfigurable="true" IsFileCollectable="true" />
<dp:TraceComponent Name="Web Setup" Description="Web Setup" IsLevelConfigurable="true"
IsFileCollectable="true" />
</dp:TraceComponentList>
</dp:ListTraceComponentsReply>
```

10.3.1.4 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/AnalysisManager/ListTraceFiles?Component/Subcomponent&Fromdate=0&ToDate=0

Reply example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<dp:ListTraceFilesReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/analysismanager">
<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>
```

- Optional URL parameter "Type" is applicable only for components that generate multiple trace types.
- URL parameters “FromDate” and “ToDate” are used to specify time range of trace files requested by user. Unified ICM components must supply these parameters.
- Attribute "Date" specifies file modification time in UTC.

- Attribute "Size" specifies file size in bytes.

10.3.1.5 DownloadTraceFile

Download the trace files that were returned by the ListTraceFiles API.

Note: Only one file may be requested at a time.

However, for trace files, the ListTraceFiles API returns one zip file (including trace files, capture files, and others). You need only one download request.

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

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/DownloadTraceFile?Component=Component/Subcomponent&File=TraceFile1.txt

Reply:

There are four possible replies:

- The server streams the specified file unzipped over the existing HTTP connection. Content (MIME) type is defined by the app server as "application/text."
- The server streams the specified file zipped over the existing HTTP connection. Content (MIME) type is defined by app server as "application/zip."
- The server streams the specified file gzipped over the existing HTTP connection. Content (MIME) type is defined by app server as "application/x-gzip."
- In case of error, app server replies error condition in following XML format (MIME type "application/xml"):

```
<?xml version="1.0" encoding="UTF-8" ?>
<dp:DownloadTraceFileReply ReturnCode="1" ErrorString="File TraceFile1.txt not found."/>
"xmlns:dp="http://www.cisco.com/vtg/analysismanager">
```

10.3.1.6 ListLogComponents

Lists all possible application components that produce log files.

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/ListLogComponents

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:ListLogComponentsReply ReturnCode="0" xmlns:dp="http://www.cisco.com/vtg/analysismanager">
<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."
/>
  <dp:LogComponent Name="Cisco ICM Diagnostic Framework Install" Description="Cisco ICM Diagnostic
Framework Install 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="Cisco CCBU Support Tools" Description="Support Tools logs" />
  <dp:LogComponent Name="Web Setup" Description="Web Setup troubleshooting and audit logs" />
  <dp:LogComponent Name="Web Agent Re-skilling" Description="Web Agent Re-skilling troubleshooting logs"
/>
</dp:LogComponentList>
</dp:ListLogComponentsReply>
```

10.3.1.7 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/AnalysisManager/ListLogFiles?Component=Component/Subcomponent&FromDate=0& ToDate=0

Reply example:

```
<?xml version="1.0" encoding="UTF-8"?>
<dp:ListLogFilesReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/analysismanager">
<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>
```

10.3.1.8 DownloadLogFile

Download the log files that were returned by the ListLogFiles API.

Note: Only one file may be requested at a time.

In the case of downloading the log files, a user may request a subsequent download with the same filename, and the exact same file is returned. This is different from the trace file because we are not deleting the log file from the server.

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/DownloadLogFile?Component=Component/Subcomponent&File=LogFile1.txt

Reply:

There are four possible replies:

- The server streams the specified file unzipped over the existing HTTP connection. Content (MIME) type is defined by the app server as "application/text."
- The server streams the specified file zipped over the existing HTTP connection. Content (MIME) type is defined by app server as "application/zip."
- The server streams the specified file zipped over the existing HTTP connection. Content (MIME) type is defined by app server as "application/x-gzip."
- In case of error, app server replies error condition in following XML format (MIME type "application/xml"):

```
<?xml version="1.0" encoding="UTF-8" ?>
<dp:DownloadLogFileReply ReturnCode="1" ErrorString="File LogFile1.txt not found."
xmlns:dp="http://www.cisco.com/vtg/analysismanager">
```

10.3.1.9 ListAppServers

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

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/ListAppServers

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:ListAppServersReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/anaysismanager">
 <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.

10.3.1.10 ListConfigurationCategories

Lists the configuration categories available on this application server.

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/ListConfigurationCategories

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:ListConfigurationCategoriesReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/analysismanager">
 <dp:Schema Version="1.0" />
 <dp:ConfigurationCategoryList>
 <dp:ConfigurationCategory Name="DumpCfg" Description="ConfigurationCategory
    for DumpCfg; Instance=ipcc8" />
 <dp:ConfigurationCategory Name="ExportICMCfg"
    Description="ConfigurationCategory for ExportICMCfg; Instance=ipcc8" />
 <dp:ConfigurationCategory Name="ConfigExport"
    Description="ConfigurationCategory for ConfigExport; Instance=ipcc8" />
 <dp:ConfigurationCategory Name="Registry" Description="ConfigurationCategory
    for Registry; Instance=ipcc8" />
```

```
</dp:ConfigurationCategoryList>
</dp:ListConfigurationCategoriesReply>
```

10.3.1.11 GetConfigurationCategory

Retrieve configuration information based on category.

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/GetConfigurationCategory?Category=????

Categories are: “DumpCfg,” “ExportICMCfg,” “ConfigExport”, and “Registry”.

Reply example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<dp:GetConfigurationCategoryReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/analysismanager">
<dp:Schema Version="1.0"/>
</dp:GetConfigurationCategoryReply>
```

The requested configuration data is returned as a zip file.

10.3.1.12 GetProductVersion

Fetches the version of the applications installed on the target server.

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/GetProductVersion

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:GetProductVersionReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/analysismanager">
<dp:Schema Version="1.0" />
<dp:ProductVersion Name="ICM" Major="8" Minor="0" Maintenance="1"
        VersionString="8.0(1) BuildNumber=26380" />
</dp:GetProductVersionReply>
```

10.3.1.13 GetProductLicense

Get license information for applications installed on target server.

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/GetProductLicense

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:GetProductLicenseReply ReturnCode="0" xmlns:dp="http://www.cisco.com/vtg/analysismanager">
<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>
```

10.3.1.14 GetPlatformInformation

Fetches server and operating system platform details.

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/GetPlatformInformation

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:GetPlatformInformationReply ReturnCode="0" xmlns:dp="http://www.cisco.com/vtg/analysismanager">
<dp:Schema Version="1.0" />
<dp:PlatformInformation>
<dp:PropertyList>
 <dp:Property Name="Host Name" Value="BUZZARDS-BAY" />
 <dp:Property Name="OS Platform" Value="Win32NT" />
 <dp:Property Name="OS Service Pack" Value="Service Pack 2" />
 <dp:Property Name="OS Version" Value="5.2.3790.131072" />
 <dp:Property Name="OS Version String" Value="Microsoft Windows NT 5.2.3790 Service Pack 2" />
 <dp:Property Name="System Directory" Value="C:\WINDOWS\system32" />
 <dp:Property Name="User Domain Name" Value="SILVERBACK" />
 <dp:Property Name="Common Language Runtime Version" Value="2.0.50727.3053" />
 <dp:Property Name="Admin Password Status" Value="3 []" />
 <dp:Property Name="Daylight Time In Effect" Value="True []" />
 <dp:Property Name="User Name" Value="[unavailable]" />
 <dp:Property Name="Computer Manufacturer" Value="HP" />
 <dp:Property Name="Model" Value="ProLiant DL380 G5" />
 <dp:Property Name="Number Of Processors" Value="[unavailable]" />
 <dp:Property Name="Total Physical Memory" Value="2145230848" />
 <dp:Property Name="Boot Device" Value="\Device\HarddiskVolume1" />
 <dp:Property Name="Build Number" Value="3790" />
 <dp:Property Name="Build Type" Value="Multiprocessor Free" />
 <dp:Property Name="Caption" Value="Microsoft(R) Windows(R) Server 2008 R2" />
 <dp:Property Name="Current Time Zone" Value="-240" />
 <dp:Property Name="IS OS a Debug version?" Value="False" />
 <dp:Property Name="Free Physical Memory" Value="653648" />
 <dp:Property Name="Free Virtual Memory" Value="2724228" />
 <dp:Property Name="Install Date" Value="Friday, February 13, 2009 3:03:50 PM" />
 <dp:Property Name="Large System Cache" Value="1 []" />
 <dp:Property Name="Locale Code" Value="0409" />
 <dp:Property Name="OS Manufacturer" Value="Microsoft Corporation" />
 <dp:Property Name="Max Process Memory Size" Value="2097024" />
 <dp:Property Name="OS Name" Value="Microsoft Windows Server 2008 R2|
C:\WINDOWS|\Device\Harddisk0\Partition1" />
 <dp:Property Name="Number Of Processes" Value="66" />
 <dp:Property Name="Number Of Users" Value="10" />
 <dp:Property Name="ServicePackMajorVersion" Value="2" />
 <dp:Property Name="ServicePackMinorVersion" Value="0" />
 <dp:Property Name="System Directory" Value="C:\WINDOWS\system32" />
 <dp:Property Name="System Drive" Value="C:" />
 <dp:Property Name="Total Virtual Memory" Value="4044744" />
 <dp:Property Name="Total Visible Memory" Value="2094952" />
 <dp:Property Name="Windows Directory" Value="C:\WINDOWS" />
</dp:PropertyList>
</dp:PlatformInformation>
</dp:GetPlatformInformationReply>
```

10.3.1.15 GetNetStat

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

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/GetNetStat?Arguments="-an"

Reply:

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

10.3.1.16 GetIPConfig

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

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/GetIPConfig?Arguments="/all"

Reply:

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

10.3.1.17 GetTraceRoute

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

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/GetTraceRoute

Reply:

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

10.3.1.18 GetPing

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

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/GetPing?Arguments="n.n.n.n"

Reply:

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

10.3.1.19 ListProcesses

Lists application processes running on the target server.

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/ListProcesses

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:ListProcessesReply ReturnCode="0" xmlns:dp="http://www.cisco.com/vtg/analysismanager">
<dp:Schema Version="1.0" />
<dp:ServiceList>
 <dp:Service Name="Cisco CCBU Support Tools NodeAgent">
  <dp:ProcessList>
   <dp:ProcessProp Name="appserver.exe" Description="appserver" />
  </dp:ProcessList>
 </dp:Service>
 <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>
```

10.3.1.20 ListServices

Lists application services running on the target server.

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/ListServices

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:ListServicesReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/ AnalysisManager">
<dp:Schema Version="1.0" />
<dp:ServiceList>
 <dp:Service Name="Cisco CCBU Support Tools NodeAgent" Description="Provides
  Support Tools communication support and processing" Status="Running"
```

```
   StartupType="Auto" LogOnAs="LocalSystem" />
  <dp:Service Name="Cisco ICM ipcc8 LoggerA" Description="Cisco ICM ipcc8
   LoggerA" Status="Running" StartupType="Auto"
   LogOnAs="SILVERBACK.CISCO.COM\IPCC8-LOGGERA-77B585" />
  <dp:Service Name="Cisco ICM ipcc8 RouterA" Description="Cisco ICM ipcc8
   RouterA" Status="Running" StartupType="Auto" LogOnAs="LocalSystem" />
  <dp:Service Name="Cisco ICM Diagnostic Framework" Description="Provides a
   web-based diagnostic service for Cisco Unified ICM, Contact Center
   Enterprise application." Status="Running" StartupType="Auto"
   LogOnAs="silverback\w2008admin" />
</dp:ServiceList>
</dp:ListServicesReply>
```

10.3.1.21 GetPerformanceInformation

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

Request:

rformanceInformation

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:GetPerformanceInformationReply ReturnCode="0" xmlns:dp="http://www.cisco.com/vtg/analysismanager">
<dp:Schema Version="1.0" />
<dp:PerformanceInformation>
<dp:PropertyList>
  <dp:Property Name="Memory/Memory Page Faults/sec" Value="29.93962" />
  <dp:Property Name="Process(_Total)/Handle Count" Value="20386" />
  <dp:Property Name="Processor(_Total)/% Processor Time" Value="13.63913" />
  <dp:Property Name="Memory/Total Memory" Value="1.399697E+09" />
  <dp:Property Name="System/Threads" Value="1165" />
  <dp:Property Name="Memory/Memory Pages/Sec" Value="3.654335" />
  <dp:Property Name="System/Processor Queue" Value="0" />
  <dp:Property Name="System/Processes" Value="73" />
  <dp:Property Name="Cisco ICM Logger(ipcc8 LoggerA)/DB Write Average Time" Value="0" />
  <dp:Property Name="Cisco ICM Logger(ipcc8 LoggerA)/DB Write Records processed" Value="0" />
  <dp:Property Name="Cisco ICM Router(ipcc8 RouterA)/Calls/sec" Value="0" />
  <dp:Property Name="Cisco ICM Router(ipcc8 RouterA)/Agents Logged On" Value="0" />
  <dp:Property Name="Cisco ICM Router(ipcc8 RouterA)/Calls In Progress" Value="0" />
  <dp:Property Name="Cisco ICM Router(ipcc8 RouterA)/Calls In Queue" Value="0" />
  <dp:Property Name="Cisco ICM Router(ipcc8 RouterA)/Router State Size(KB)" Value="0" />
  <dp:Property Name="Cisco ICM Router(ipcc8 RouterA)/Messages Processed/sec" Value="0" />
  <dp:Property Name="Cisco ICM Router(ipcc8 RouterA)/Bytes Processed/sec" Value="0" />
  <dp:Property Name="Cisco ICM Router(ipcc8 RouterA)/Avg Process Time/Message (ms)" Value="0" />
  <dp:Property Name="Cisco ICM Router(ipcc8 RouterA)/Max Process Time(ms)" Value="0" />
  <dp:Property Name="Cisco ICM Router(ipcc8 RouterA)/Calls In Router" Value="0" />
</dp:PropertyList>
</dp:PerformanceInformation>
</dp:GetPerformanceInformationReply>
```

10.3.1.22 GetPerfCounterValue

Get the current value of a performance counter from the target server.

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/GetPerfCounterValue?CategoryName=Processor&CounterName=”%Processor Time”&PerfInstance=”_Total”

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:GetPerfCounterValueReply ReturnCode="0" xmlns:dp="http://www.cisco.com/vtg/analysismanager">
<dp:Schema Version="1.0" />
<dp:PerformanceInformation>
<dp:PropertyList>
  <dp:Property Name="CategoryName" Value="Processor" />
  <dp:Property Name="CounterName" Value="% Processor Time" />
  <dp:Property Name="InstanceName" Value="_Total" />
  <dp:Property Name="BaseValue" Value="0" />
  <dp:Property Name="CounterFrequency" Value="0" />
  <dp:Property Name="CounterTimeStamp" Value="0" />
  <dp:Property Name="CounterType" Value="Timer100NsInverse" />
  <dp:Property Name="RawValue" Value="203276171875" />
  <dp:Property Name="NextValue" Value="0.003199898" />
  <dp:Property Name="SystemFrequency" Value="2333380000" />
  <dp:Property Name="TimeStamp" Value="48917923479390" />
  <dp:Property Name="TimeStamp100nSec" Value="128929442042854145" />
</dp:PropertyList>
</dp:PerformanceInformation>
</dp:GetPerfCounterValueReply>
```

10.3.1.23 GetAlarms

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

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/GetAlarms?Severity=#?Count=##

"Severity" and "Count" are optional parameters.

Severity may be a numeric value between 1 and 3 (1=Informational, 2=Warning, 3=Error) – returns all alarms with a severity greater-than or equal-to the specified severity.

Count may be a numeric value between 1 and 25 – 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/analysismanager">
<dp:Schema Version="1.0" />
<dp:AlarmList>
  <dp:Alarm DateTime="Jul 24, 2009 15:41:41 +0000" Type="Clear" Id="1028104" Severity="1"
Instance="ipcc8" Component="4_5_BERKSHIRE_ICM\ipcc8\LoggerB" SubComponent="nm"
Message="ICM\ipcc8\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="ipcc8" 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="ipcc8" 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="ipcc8" 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="ipcc8" 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="ipcc8" Component="4_1_BERKSHIRE_ICM\ipcc8\RouterB" SubComponent="nm"
Message="ICM\ipcc8\RouterB Node Manager started. Last shutdown was for reboot afterfailure of critical
process." />
```

<dp:Alarm DateTime="Jul 24, 2009 15:41:13 +0000" Type="Clear" Id="10500FF" Severity="1" Instance="ipcc8" 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="ipcc8" 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="ipcc8" 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="ipcc8" 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="ipcc8" 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="ipcc8" 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="ipcc8" 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="ipcc8" 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="ipcc8" 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="ipcc8" 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="ipcc8" Component="24_1_B_dba" SubComponent="rtr" Message="Side B dba process is OK." />
<dp:Alarm DateTime="Jul 24, 2009 15:42:18 +0000" Type="Clear" Id="1040023" Severity="1" Instance="ipcc8" Component="5_1_0" SubComponent="mds" Message="Communication with peer Synchronizer established." />
<dp:Alarm DateTime="Jul 24, 2009 15:37:55 +0000" Type="Clear" Id="1028103" Severity="1" Instance="ipcc8" Component="4_4_WACHUSETT_ICM\ipcc8\Distributor" SubComponent="nm" Message="ICM\ipcc8\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="ipcc8" Component="3_4_WACHUSETT_ICM\ipcc8\Distributor_uaw" SubComponent="nm" Message="ICM\ipcc8\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="ipcc8" Component="3_4_WACHUSETT_ICM\ipcc8\Distributor_uaw" SubComponent="nm" Message="ICM\ipcc8\Distributor node restarting process uaw after having delayed restart for 1 seconds." />
<dp:Alarm DateTime="Jul 24, 2009 15:37:39 +0000" Type="Raise" Id="102C10F" Severity="2" Instance="ipcc8" Component="3_4_WACHUSETT_ICM\ipcc8\Distributor_uaw" SubComponent="nm" Message="Process uaw on ICM\ipcc8\Distributor is down after running for 30 seconds. It will restart after delaying 1 second for related operations to complete." />
<dp:Alarm DateTime="Jul 24, 2009 15:37:39 +0000" Type="Raise" Id="102C10E" Severity="3" Instance="ipcc8" Component="3_4_WACHUSETT_ICM\ipcc8\Distributor_uaw" SubComponent="nm" Message="Process uaw on ICM\ipcc8\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="ipcc8" Component="3_4_WACHUSETT_ICM\ipcc8\Distributor_rpl" SubComponent="nm" Message="ICM\ipcc8\Distributor node process rpl successfully started." />
<dp:Alarm DateTime="Jul 24, 2009 15:37:13 +0000" Type="Clear" Id="102C111" Severity="1" Instance="ipcc8" Component="3_4_WACHUSETT_ICM\ipcc8\Distributor_rtc" SubComponent="nm" Message="ICM\ipcc8\Distributor node process rtc successfully started." />
</dp:AlarmList>
</dp:GetAlarmsReply>

10.3.1.24 SetAlarms

Turns Unified CCE alarming OFF or ON. Turning alarming OFF is useful during maintenance windows to prevent flooding at the management station.

Request:

https://<server>:<port>/icm-dp/rest/AnalysisManager/SetAlarms?State=ON/OFF

Reply example:

```
<?xml version="1.0" encoding="utf-8" ?>
<dp:SetAlarmsReply ReturnCode="0"
xmlns:dp="http://www.cisco.com/vtg/analysismanager">
<dp:Schema Version="1.0" />
</dp:SetAlarmsReply>
```

10.4 Diagnostic Framework Troubleshooting

The Diagnostic Framework is self contained and does not require any additional configuration other than assigning users. If you encounter any issues with the service, see the following table:

Table 10-11: Diagnostic Framework Troubleshooting

Issue	Troubleshooting / Remedy
Diagnostic Framework service does not start	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. Make sure none of the configuration files is missing. Check Event Viewer and Diagnostic Framework log file for any initialization errors.
Cannot access any API from the client, such as Internet Explorer	Confirm the base URL is correct; compare it with the URL in the service configuration file DiagFwSvc.exe.config. Confirm the API used is valid; try accessing the built in GetMenu API. Make sure the API is accessed using HTTPS. Make sure the credentials used as valid, check Windows Event log for any authentication errors and Diagnostic Framework log for any authorization errors. Use DiagFwCertMgr utility to validate the certificate binding to the port in use. Recreate or rebind the certificate if any issues were found. If using Internet Explorer, clear the cache and restart the browser. 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.
Some commands work, and others do not seem to work.	Ensure that you use an approved browser. Currently only Internet Explorer 7 and 8 are approved.

10.5 DUMPLOG

Using the DUMPLOG Utility Optional Cisco Log Message Format

The DUMPLOG utility converts binary log files written by Unified ICM/Unified CCE processes into readable text format. An enhancement was added to DUMPLOG with Release 7.2(1) of the Unified ICM/Unified CCE to optionally display the binary log files in Cisco Log message format. For more information about the Cisco Log format, see section 5.1. For more information about this utility, see the *How to Use the DumpLog Utility* Tech Note in

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_tech_notes_list.html

Header

Cisco Log formatted log entries include a more comprehensive header compared to DUMPLOG standard format.

DumpLog Standard Format

Standard formatted DUMPLOG entries display the following fields:

<TIMESTAMP> <COMPONENT-PROCESS> <MESSAGE>

The timestamp is represented as a 24-hour value (hh:mm:ss). It does not include the date, which appears on a separate line at the beginning of the file and when a new day starts. For example:

Events from February 8, 2007
00:37:44 ra-rtr MDS is in service.

Cisco Log Format

Cisco Log formatted DUMPLOG entries display the following fields:

<SEQNUM>: <HOST>: <TIMESTAMP> <TIMEZONE>: %APPNAME: %<TAGS>:<MESSAGE>

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=ipcc][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 10-12: APPNAME and TAGS Used in DUMPLOG Trace Output

Field	Description
APPNAME	PRODUCT_COMPONENT_MESSAGECATEGORY PRODUCT - always ICM COMPONENT – such as Router MESSAGECATEGORY – such as ProcessSynchronization
TAGS	Acceptable tags are: [comp=%s] - component name including side, such as Router A [pname=%s] - process name, such as rtr

	[iid=%s] - instance name, such as ipcc [sev=%s] – severity, such as info and optionally [part=%1.%2/%3], which is used only for multi-line entries as described later in this section.

Timestamp

The timestamp displayed in DUMPLOG standard format is in local time relative to the server on which DUMPLOG is run. The timestamp displayed in Cisco Log format is in GMT time independent of the server on which DUMPLOG is run.

Note: Date/time options specified on the command line are entered in local time, regardless of whether the Cisco Log option is selected. Therefore, timestamps displayed as part of the Cisco Log formatted entry might appear to be outside of the date/time range selected.

Multi-line Entries

The message portion of some DUMPLOG entries might contain one or more embedded new line characters ('\n'), which cause the messages to appear on multiple lines and might also include blank lines. This is especially true for entries that contain statistics.

For a DUMPLOG standard formatted message, only the first line contains the header field as shown in the following example:

```
00:36:09 ra-nm ICM\ipcc\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 as shown in the following example.

```
19: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown: [comp=Router-
A][pname=nm][iid=ipcc][sev=info][part=19.1/14]: ICM\ipcc\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=ipcc][sev=info][part=19.2/14]: Process name: ccag

21: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown: [comp=Router-
A][pname=nm][iid=ipcc][sev=info][part=19.3/14]: Process status ACTIVE

22: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown: [comp=Router-
A][pname=nm][iid=ipcc][sev=info][part=19.4/14]: Process ID 6c0

23: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown: [comp=Router-
A][pname=nm][iid=ipcc][sev=info][part=19.5/14]: Number of times process started 1

24: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown: [comp=Router-
A][pname=nm][iid=ipcc][sev=info][part=19.6/14]: Last start time: 00:35:31 2/8/2007
```

25: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown: [comp=Router-A][pname=nm][iid=ipcc][sev=info][part=19.7/14]: Pings completed in zero time: 0

26: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown: [comp=Router-A][pname=nm][iid=ipcc][sev=info][part=19.8/14]: Pings completed in first third: 0

27: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown: [comp=Router-A][pname=nm][iid=ipcc][sev=info][part=19.9/14]: Total first third milliseconds: 0

28: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown: [comp=Router-A][pname=nm][iid=ipcc][sev=info][part=19.10/14]: Pings completed in second third: 0

29: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown: [comp=Router-A][pname=nm][iid=ipcc][sev=info][part=19.11/14]: Total second third milliseconds: 0

30: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown: [comp=Router-A][pname=nm][iid=ipcc][sev=info][part=19.12/14]: Pings completed in third third: 0

31: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown: [comp=Router-A][pname=nm][iid=ipcc][sev=info][part=19.13/14]: Total third third milliseconds: 0

32: CICMRGRA: Feb 8 2007 05:36:09.890 +0000: %ICM_Router_unknown: [comp=Router-A][pname=nm][iid=ipcc][sev=info][part=19.14/14]: Longest Ping Time: 0

To differentiate each line in the entry, the part tag is added to each header where:

[part=#1.#2/#3]

#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, [part=19.14/14]:

#1 = 19. #2 = 14 / #3 = 14

10.6 EMSMON

In Release 8.5(2), for Windows 2008, process windows for Unified CCE processes are no longer available. The title bar status information is available in the Diagnostic Portico; however, real time messages do not appear there. To address this, Cisco recommends that partners and TAC use EMSMON as a replacement.

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 processs 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.

10.6.1 How to Run EMSMON

You can start EMSMON at anytime, even when the process is not running. (You can have a batch file on a machine to start sessions.) If the process is down, EMSMON displays messages from the process when the process starts. EMSMON does not end when the process ends. To end EMSMON, press Ctrl+C or close the window.

EMSMON has the same parameters as ProcMon:

<instance> <node> <process> [<process>…] [<system>]

The system parameter is optional. Use the system parameter to remotely run EMSMON.

For example, if the instance node is "ucce," to monitor the JTAPI gateway on PG1A, type the following:

EMSMON ucce PG1A jgw1

If you are remote (on another PG) and the system name is UCCEPG1A, type:

EMSMON ucce PG1A jgw1 UCCEPG1A

Note: A trust relationship must exist between the two machines. (Use the "NET USE" command or complete an operation that sets up a trust [for example, map a drive].)

10.6.2 Monitoring Process

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

Multiple EMSMONs can watch a single process. For example, you can have a local EMSMON and a remote EMSMON. However, Cisco recommends that you use one EMSMON only for each process.

10.6.3 Running EMSMON Remotely

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

To run EMSMON on a remote machine, copy emsmon.exe, emsmon.pdb, and icrmessages.dll from c:\icm\bin and place them on a remote machine.

10.6.4 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 following message "You are being disconnected because another user has connected to this named pipe."

If your system is running a heavy call load, your EMSMON connections may disconnect and the following message appears: "You are being disconnected because the system is running a heavy call load; this connection may impact the performance of the system. It is recommended that you do not reconnect your EMSMON sessions until your system returns to a normal call load."

Note: To prevent Unified CCE processes from exceeding the system memory, Unified CC processes may stop sending queued event messages to slow or paused EMSMON clients. If this occurs, EMSMON clients display a message indicating one of the clients fell behind and there is a gap. This message is also logged in the processes event log. This can happen if a particular EMSMON client is too slow or paused by quick edit or Ctrl+S for example. This does not affect the Unified CCE process, only the EMSMON client.

11 Appendix A - 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 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 Unified Contact Center 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 Contact Center
cccaVersion.0 = 7.1(1)
cccaTimeZoneName.0 = Eastern Standard Time
cccaTimeZoneOffsetHours.0 = 5
cccaTimeZoneOffsetMinutes.0 = 0
cccaSupportToolsURL.0 =
cccaInstanceName.0 = acme
cccaComponentType.0.1 = router(1)
cccaComponentType.0.2 = logger(2)
cccaComponentType.0.3 = pg(4)
cccaComponentType.0.4 = distAW(3)
cccaComponentName.0.1 = RouterA
cccaComponentName.0.2 = LoggerA
cccaComponentName.0.3 = PG1A
cccaComponentName.0.4 = Distributor
cccaComponentStatus.0.1 = started(4)
cccaComponentStatus.0.2 = started(4)
cccaComponentStatus.0.3 = started(4)
cccaComponentStatus.0.4 = started(4)
cccaComponentElmtName.0.1.1 = ccagent
cccaComponentElmtName.0.1.2 = crspnic
cccaComponentElmtName.0.1.3 = dbagent
cccaComponentElmtName.0.1.4 = mdsproc
cccaComponentElmtName.0.1.5 = router
cccaComponentElmtName.0.1.6 = rtsvr
cccaComponentElmtName.0.1.7 = testsync
cccaComponentElmtName.0.2.8 = configlogger
cccaComponentElmtName.0.2.9 = csfs
cccaComponentElmtName.0.2.10 = histlogger
cccaComponentElmtName.0.2.11 = recovery

cccaComponentElmtName.0.3.12 = mdsproc
cccaComponentElmtName.0.3.13 = opc
cccaComponentElmtName.0.3.14 = pgagent
cccaComponentElmtName.0.3.15 = acmipim
cccaComponentElmtName.0.3.16 = testsync
cccaComponentElmtName.0.4.17 = configlogger
cccaComponentElmtName.0.4.18 = rtclient
cccaComponentElmtName.0.4.19 = rtdist
cccaComponentElmtName.0.4.20 = updateaw
cccaComponentElmtRunID.0.1.1 = 3336
cccaComponentElmtRunID.0.1.2 = 2992
cccaComponentElmtRunID.0.1.3 = 3600
cccaComponentElmtRunID.0.1.4 = 3920
cccaComponentElmtRunID.0.1.5 = 4040
cccaComponentElmtRunID.0.1.6 = 3532
cccaComponentElmtRunID.0.1.7 = 4100
cccaComponentElmtRunID.0.2.8 = 948
cccaComponentElmtRunID.0.2.9 = 3248
cccaComponentElmtRunID.0.2.10 = 1248
cccaComponentElmtRunID.0.2.11 = 3272
cccaComponentElmtRunID.0.3.12 = 4724
cccaComponentElmtRunID.0.3.13 = 4864
cccaComponentElmtRunID.0.3.14 = 4964
cccaComponentElmtRunID.0.3.15 = 5236
cccaComponentElmtRunID.0.3.16 = 5228
cccaComponentElmtRunID.0.4.17 = 5460
cccaComponentElmtRunID.0.4.18 = 5488
cccaComponentElmtRunID.0.4.19 = 5504
cccaComponentElmtRunID.0.4.20 = 5536
cccaComponentElmtStatus.0.1.1 = active(5)
cccaComponentElmtStatus.0.1.2 = started(4)
cccaComponentElmtStatus.0.1.3 = active(5)
cccaComponentElmtStatus.0.1.4 = active(5)
cccaComponentElmtStatus.0.1.5 = active(5)
cccaComponentElmtStatus.0.1.6 = active(5)
cccaComponentElmtStatus.0.1.7 = active(5)
cccaComponentElmtStatus.0.2.8 = active(5)
cccaComponentElmtStatus.0.2.9 = active(5)
cccaComponentElmtStatus.0.2.10 = active(5)
cccaComponentElmtStatus.0.2.11 = active(5)
cccaComponentElmtStatus.0.3.12 = active(5)
cccaComponentElmtStatus.0.3.13 = active(5)
cccaComponentElmtStatus.0.3.14 = active(5)
cccaComponentElmtStatus.0.3.15 = standby(6)
cccaComponentElmtStatus.0.3.16 = active(5)
cccaComponentElmtStatus.0.4.17 = active(5)
cccaComponentElmtStatus.0.4.18 = active(5)
cccaComponentElmtStatus.0.4.19 = active(5)
cccaComponentElmtStatus.0.4.20 = active(5)
cccaRouterSide.0.1 = sideA(1)
cccaRouterCallsPerSec.0.1 = 0
cccaRouterAgentsLoggedOn.0.1 = 0
cccaRouterCallsInProgress.0.1 = 0
cccaRouterDuplexPairName.0.1 = cc-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)
cccaDistAwWebViewServerName.0.4 =
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

12 Appendix B – Unified ICM/Unified CCE SNMP Notifications

Notes:

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" label (where 'n' is a numeric value) indicates a substitution field whereby node-specific or process-specific information is inserted.

Table 12-1: SNMP Notifications

MsgID (in hex)	Type	Severity	Message Text	
Description				**Action**
1028101	Clear	Warning	%1 Node Manager initializing.	
The node management library, common to nearly all ICM processes, is initializing itself. This is standard practice when a process (re)starts.				No action is required.
1028103	Clear	Informational	%1 Node Manager started. Last shutdown was by operator request.	
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.				No action is required.
1028104	Clear	Informational	%1 Node Manager started. Last shutdown was due to system shutdown.	
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.				No action is required.
1028105	Raise	Warning	The operator/administrator has shutdown the ICM software on %1.	
Node Manager on the ICM node was 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.				Contact the operator/administrator to determine the reason for the shutdown.
1029101	Clear	Informational	%1 Node Manager Manager started.	
The Node Manager Manager process (which oversees the Node Manager process) has started.				No action is required.
102C101*	Raise	Error	%1 node critical process %2 died. Rebooting node.	
A critical process needed to run the ICM software on this node has died. The Node Manager is forcing a reboot of the node.				Contact the Support Center.
102C103*	Clear	Warning	%1 node restarting process %2.	
The Node Manager is restarting process %2 after the process died or was terminated.				No action is required.
102C107*	Clear	Informational	%1 Node Manager started. Last shutdown was for reboot after failure of critical process.	
The Node Manager has started. The last shutdown was requested by the Node Manager because it recognized that a critical process for the node failed.				No action is required.
102C108*	Clear	Error	%1 Node Manager started. Last shutdown was for unknown reasons. Possible causes include a power failure, a system failure or a Node Manager exit.	
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.				Contact the Support Center.
102C109*	Raise	Warning	%4 node process %5 exited after %1 seconds. Minimum required uptime for %5 process is %2 seconds. Delaying process restart for %3	

			seconds.
Process %5 exited after running for %1 seconds. Such processes must run for at least %2 seconds before the Node Manager automatically restarts them after they terminate. The Node Manager restarts the process after delaying %3 seconds for other environmental changes to complete.			No action is required.
102C10A*	Clear	Warning	%2 node restarting process %3 after having delayed restart for %1 seconds.
The Node Manager is restarting process %3 after the requisite delay of %1 seconds.			No action is required.
102C10B*	Raise	Error	Terminating process %2.
The %1 Node Manager is terminating process %2.			No action is required.
102C10C*	Raise	Error	%1 node process %2 exited after having detected a software failure.
Process %2 exited (terminated itself) after it detected an internal software error.			If the process continues to terminate itself, call the Support Center.
102C10D*	Raise	Warning	Process %2 on %1 has detected a failure. Node Manager is restarting the process.
The specified Process 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).			Node Manager on the ICM node restarts the process. The node should be checked to assure it is online using rttest. If the condition is common, the process logs must be examined for cause.
102C10E*	Raise	Error	Process %2 on %1 went down for unknown reason. Exit code %3. It automatically restarts.
The specified Process exited (terminated) with the indicated exit code. This termination is unexpected and the process died for an unknown reason. It automatically restarts.			Contact the Support Center.
102C10F*	Raise	Warning	Process %4 on %3 is down after running for %1 seconds. It restarts after delaying %2 seconds for related operations to complete.
Specified process is down after running for the indicated number of seconds. It restarts after delaying for the specified number of seconds for related operations to complete.			Determine if process returned to service or stayed offline. If process is offline or bouncing determine the cause from logs.
102C110*	Clear	Warning	%1 node process %2 successfully reinitialized after restart.
Process %2 was successfully restarted.			No action is required.
102C111*	Clear	Informational	%1 node process %2 successfully started.
Process %2 was successfully started.			No action is required.
102C112*	Raise	Warning	%1 node process %2 exited cleanly and requested that it be restarted by the Node Manager.
Process %2 terminated itself successfully and requested that the Node Manager restart it.			No action is required.
102C113	Raise	Warning	%1 node process %2 exited from Control-C or window close.
Process %2 exited because of a CTRL-C request or a request to close the process's active window.			No action is required.
102C114*	Raise	Error	%1 node process %2 exited and requested that the Node Manager reboot the system.
Process %2 terminated itself successfully but, due to other conditions, requested that the Node Manager reboot the machine.			No action is required.
102D101*	Raise	Error	%3 Node Manager exited after having been up for %1 seconds. Scheduling system reboot in %2 seconds.
The Node Manager itself exited after having run for %1 seconds. The			Contact the Support Center.

machine restarts after waiting %2 seconds.				
102D102*	Raise	Error	%2 Node Manager exited after having been up for %1 seconds. Auto-reboot is disabled. Will attempt service restart.	
The Node Manager itself exited after having run for %1 seconds. The machine cannot be rebooted because auto-reboot is disabled. The Node Manager Manager attempts to restart the service.				Contact the Support Center.
102D103*	Raise	Error	%3 Node Manager requested reboot after having been up for %1 seconds. Scheduling system reboot in %2 seconds.	
The Node Manager requested the machine be rebooted after having run for %1 seconds. The machine restarts after waiting %2 seconds.				Contact the Support Center.
102D104*	Raise	Error	%2 Node Manager requested reboot after having been up for %1 seconds. Auto-reboot is disabled. Will attempt service restart.	
The Node Manager requested the machine be rebooted after having run for %1 seconds. The machine cannot be rebooted because auto-reboot is disabled. The Node Manager Manager attempts to restart the service.				Contact the Support Center.
102D105*	Raise	Error	%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.	
A Critical Process requested a reboot after the service has been up for %1 seconds. The machine cannot be rebooted because Auto-reboot on Process Request is disabled. The Node Manager Manager attempts to restart the service.				Contact the Support Center.
102D106*	Raise	Error	%3 A Critical Process has requested a reboot after having been up for %1 seconds. Scheduling system reboot in %2 seconds.	
A Critical Process requested the machine be rebooted after having run for %1 seconds. The machine restarts after waiting %2 seconds.				Contact the Support Center.
1040010*	Raise	Warning	Synchronizer timed out trying to establish connection to peer.	
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.				Verify reliable network connectivity on the private network. Call the Cisco Systems, Inc. Customer Support Center for a software failure on the duplexed partner.
1040022*	Raise	Error	Connectivity with duplexed partner has been lost due to a failure of the private network, or duplexed partner is out of service.	
The MDS message synchronizer lost connectivity to its duplexed partner. This indicates either a failure of the private network, or a failure of the duplexed partner.				Confirm services are running on peer machine. Check MDS process to determine if it is paired or isolated. Ping test between peers over the private network. Check PGAG and MDS for TOS (Test Other Side) messages indicating the private network has failed and MDS is testing the health of the peer over the public network.
1040023*	Clear	Informational	Communication with peer Synchronizer established.	
The MDS message synchronizer has established communication with its duplexed partner.				No action is required.
104802A	Single-state Raise	Warning	MDS Time Delivery Queue size is increasing, current size is %1, but will continue to send messages.	
MDS Time Delivery Queue size is increasing over time.				Ensure that the ICM/IPCC configuration (# agents, # skills/agent, # PGs) is within the supported limit.
105007D*	Clear	Informational	Peripheral %2 (ID %1) is on-line.	
The specified peripheral is on-line to the Unified ICM. Call and agent state information is being received by the Router for this site.				No action is required.

105007E*	Raise	Error	ACD/IVR %2 (ID %1) is off-line and not visible to the Peripheral Gateway. Routing to this site is impacted.
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.			If Peripheral Gateway is also offline per messaging (message ID 10500D1) or 'rttest' result, then first proceed with troubleshooting for Peripheral Gateway off-line alarm. Otherwise ACD/IVR Vendor should be contacted for resolution.
10500D0*	Clear	Informational	Physical controller %2 (ID %1) is on-line.
The Router is reporting that physical controller %2 is on-line.			No action is required.
10500D1*	Raise	Error	Peripheral Gateway %2 (ID %1) is not connected to the Central Controller or is out of service. Routing to this site is impacted.
The specified Peripheral Gateway is not connected to the Central Controller. It could be down. Possibly it was taken out of service. Routing to this site is impacted.			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.
10500D2*	Clear	Informational	PG has reported that peripheral %2 (ID %1) is operational.
PG reported that peripheral %2 (ID %1) is operational.			No action is required.
10500D3*	Raise	Error	PG has reported that peripheral %2 (ID %1) is not operational.
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.			Check that the peripheral is not off-line and that the connection from the peripheral to the PG is intact.
10500F6	Raise	Informational	ScriptTable %2 (ID %1) is available only on side A.
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.			Configure a ScriptTable on side B that is identical to that on side A.
10500F7	Raise	Informational	ScriptTable %2 (ID %1) is available only on side B.
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.			Configure a ScriptTable on side B that is identical to that on side A.
10500F8	Raise	Error	ScriptTable %2 (ID %1) is not available on either side.
No DB Lookup requests can be processed as ScriptTable %2 is unavailable on either side of the central controller.			Configure a ScriptTable on either side A or side B, preferably both.
10500F9	Clear	Informational	ScriptTable %2 (ID %1) is available on both sides A & B.
ScriptTable %2 is configured on both sides of the central controller.			No action is required.
10500FF*	Clear	Informational	Side %1 %2 process is OK.
The Router is reporting that side %1 process %2 is OK.			No action is required.
1050100*	Raise	Error	Process %2 at the Central Site side %1 is down.
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.			No action is required.

10501F1*	Clear	Informational	ICM Node %2 (ID %1) is on-line.	
The specified node is on-line to the Unified ICM.				No action is required.
10501F2*	Raise	Error	ICM Node %2 (ID %1) is off-line.	
The specified node is not visible to the Unified ICM. Distribution of real time data may be impacted.				No action is required.
10501F6	Clear	Informational	The Router's state size of %1 mb is now below the alarm limit of %2 mb.	
The Router's state size of %1 mb is now below the alarm limit of %2 mb.				No action is required.
10501F7	Raise	Error	The Router's state size of %1 mb has grown beyond the alarm limit of %2 mb.	
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.				The alarm limit can be raised with the 'rtsetting' tool.
10501F8*	Clear	Informational	ICM Node %2 (ID %1) on system %3 is on-line.	
The specified node is on-line to the Unified ICM.				No action is required.
10501F9*	Raise	Error	ICM Node %2 (ID %1) on system %3 is off-line.	
The specified node is not visible to the Unified 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.				Check the communication paths that connect the Router and the node.
10501FD	Clear	Informational	The Router has completed loading the initial configuration from the Logger.	
The specified node is on-line to the Unified ICM.				No action is required.
10501FE	Raise	Error	The Router has not loaded a configuration from the Logger.	
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.				Check the communication paths that connect the Router and the node.
105023C*	Single-state Raise	Error	The Router has detected that it is no longer synchronized with its partner.	
The Router detected that it is no longer synchronized with its partner. One result of this is that the Router might be routing some calls incorrectly.				Recommended 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 are in sync.
106003A	Raise	Error	World Wide Web Publishing Service may be down. ICM cannot communicate with web server.	
World Wide Web Publishing Service may be down. The Unified ICM cannot communicate with web server.				Start World Wide Web Publishing Service if it is not running. Otherwise, look for messages in the IIS error log.
106003B	Clear	Informational	World Wide Web Publishing Service is up.	
World Wide Web Publishing Service is up.				No action is required.
108C020*	Clear	Informational	The Enterprise CTI Server associated with this Peripheral Gateway is on-line on %1.	
The Enterprise CTI server associated with this Peripheral Gateway is on-line. Enterprise				No action is required.

CTI Client applications can connect to the server and exchange call and agent data.				
108C021*	Raise	Error	The Enterprise CTI server associated with this Peripheral Gateway is down.	
The Enterprise CTI server associated with this Peripheral Gateway is off-line. Enterprise CTI Client applications cannot connect to the server and exchange call and agent data.				Look at the CTI server events and logs.
10D800A	Raise	Error	SS7 linkset %1 unavailable.	
The specified SS7 linkset to the AT&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&T network are not operational. This is most likely due to a circuit problem in either the Local Exchange Carrier or in the AT&T network. Other possible causes include equipment problems and maintenance procedures. Because 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 is also generated.				Occasional brief outages of a single link (and hence a single linkset) are not unusual and require no action. If the outage persists for more than five minutes, or if the outage occurs frequently, contact the AT&T Advanced Features Services Center (AFDSC) at 800-621-6901. Ask to speak to an ICP technician.
10D800B	Clear	Informational	SS7 linkset %1 available.	
The specified SS7 linkset to the AT&T network is now in a working state.				No action is required.
10D8010	Clear	Informational	SS7 network accessible. DPC=%1	
The interface to the AT&T network returned to a working state. At least one link is now operational, although others may still be down.				No action is required.
10D8011	Raise	Error	SS7 network inaccessible. DPC=%1	
All links to the AT&T network from the NIC originating this event are in a non-working state. If the links are not provisioned with physical diversity, then this outage could arise from a single circuit failure in the Local Exchange Carrier or in the AT&T network. Failure of equipment common to all links is another possible cause, for example, 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.				Verify that you do not have an equipment failure at your site that could cause this problem. If the outage persists for more than five minutes, or if the outage occurs frequently, contact the AT&T Advanced Features Service Center (AFSC) at 800-621-6901. Ask to speak to an ICP technician. If you have provisioned alternate A-links, use your AT&T network routing application, for example, Routing Manager, to redirect traffic to the alternate CRP which uses the alternate links.
10D8101	Clear	Informational	ICP Gateway ONLINE.	
The NIC Gateway entered the online state. The Routing Clients must now be configured, started, and brought online for the NIC to become fully operational. This sequence automatically proceeds.				No action is required.
10D8102	Raise	Error	NIC ICP Gateway has stopped operation due to the following \ error (%1). Calls will be default routed.	
The NIC ICP Gateway stopped operation due to the specified error code. Calls are 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.				No action is required.
10D8106	Raise	Error	Routing Client %1 STOPPED. (%2)	
The specified Routing Client stopped operation for the specified reason code. Calls for the associated subsystem/CRP-ID are 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.				This event can be caused by a transient problem that may be automatically corrected. If the problem persists for more than five minutes, contact the Customer Service Center.
10D8107	Clear	Informational	Routing Client %1 ONLINE.	

The specified Routing Client is now fully operational and able to process calls for the associated subsystem/CRP-ID.				No action is required.
10F8004	Clear	Informational	Device %1 path changing to idle state.	
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).				No action is required.
10F8005	Clear	Informational	Device %1 path changing to active state.	
The indicated device is using this side of the Central Controller for its active communication path.				No action is required.
10F8007	Raise	Error	Device %1 path realignment failed.	
The indicated device failed to realign its message stream to this side of the Central Controller.				No action is required.
10F8008	Raise	Error	Device %1 disconnected.	
The indicated device is disconnected from this side of the Central Controller. This may be caused by a network problem or device failure.				Remedy network problems, if any. Call the Cisco Systems, Inc. Customer Support Center for a software failure on the device.
10F800E	Raise	Warning	Device %1 path reset.	
The communication path between this side of the Central Controller and the indicated device is reset to an initial state.				No action is required.
10F800F	Clear	Informational	Device %1 initializing message stream.	
The indicated device is initializing its message stream with this side of the Central Controller.				No action is required.
10F801D	Raise	Warning	The Network communications between ICM Router and Peripheral Gateway or NIC %2 has been down for %1 minutes.	
No communication path from the indicated device to this side of the Central Controller existed for the indicated time period. This indicates either an extended network outage or an extended outage at the device.				One or more network links between the named device and the named side of the ICM Router 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.
110800A	Clear	Informational	RDG %1 (%2) is now accessible.	
The MCI NIC established its first communication session with the indicated MCI Remote Data Gateway. This indicates that network connectivity exists to the indicated RDG.				No action is required.
110800B	Raise	Error	The MCI Remote Data Gateway (RDG) %1 (%2) is either out of service or communications between ICM and the RDG has broken.	
The MCI NIC no longer has any communication sessions established with the indicated MCI Remote Data Gateway. This points to a problem with the indicated RDG, or a problem with network connectivity.				The connection between the Router and MCI failed. If all Remote Data Gateways (RDGs) are disconnected from the Router then ICM is not routing calls. MCI should be contacted for resolution.
1108200	Clear	Informational	MCIGATE ONLINE.	
The MCI NIC is online and is prepared to accept route requests from the MCI network.				No action is required.
1108201	Raise	Error	MCIGATE OFFLINE.	
The MCI NIC is offline and cannot accept route requests from the MCI network.				No action is required.

1168200	Clear	Informational	SPRGATE ONLINE.	
SPRCommStart(), which begins execution of the Gateway has returned without error.				No action is required.
1168201	Raise	Error	SPRGATE OFFLINE.	
SPRGate is halting execution.				No action is required.
116C100	Clear	Informational	SPRCOMM Link %1 to SCP %2 OPEN.	
The Link State is changing from LINK_OPENING to LINK_OPEN.				No action is required.
116C101	Raise	Error	The Sprint Service Control Point (SCP) %1 to (%2) is either out of service or communications between ICM and the SCP has broken.	
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.				The connection between the Router and Sprint failed. If all Service Control Points (SCPs) are disconnected from the Router then ICM is not routing calls. Sprint should be contacted for resolution.
118C002	Single-state Raise	Informational	%1%% of the available free space is used in %2 database.	
%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 begins deleting the oldest historical records from the database.				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.
118C00C	Single-state Raise	Informational	%1%% of the available log space is used in %2 database.	
%1%% of the available log space is used in %2 database.				No action is required.
118C00F	Raise	Warning	Begin Automatic Purge: %1%% of the available data space is used in the %2 database.	
Automatic Purge is being run 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.				Contact the Support Center.
118C010	Clear	Warning	Automatic Purge Complete: %1%% of the available data space is used in the %2 database.	
Automatic Purge has been run to keep the database from running out of space. The parameters for the daily purge must be adjusted to match the database storage capacity.				No action is required.
118C015	Clear	Informational	Connected To Client system %1 on port %2.	
Logger successfully connected to a client system.				No action is required.
118C017	Raise	Informational	Logger or HDS connection to client system %1 on port %2 either went out of service or has been broken.	
Logger or HDS on the specified TCP/IP connection and port number either went out of service or communication is broken.			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.	
118C033	Single-state Raise	Warning	Cannot find Routing Client with NetworkRoutingClient %1 on Server %2 in Database %3, Unable to Replicate Data to Customer %4 on CICR Instance %5	
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 cannot complete the replication in this case.				No action is required.

118C034	Single-state Raise	Warning	Cannot find Customer %1 or Instance %2 on Server %3 in Database %4. Unable to Replicate to Customer %1 on CICR Instance %2
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.			No action is required.
118C035	Single-state Raise	Warning	Dialed Number or Label Exists with Duplicate Key on Server %1 in Database %2, Unable to Replicate to Customer %3 on CICR Instance %4
CICR Replication found that inserting the Dialed Number or Label causes a Duplicate Key error. Therefore the Dialed Number or Lable cannot be inserted. CICR Replication cannot complete the replication in this case.			No action is required.
118C036	Single-state Raise	Warning	Duplicate Key Exists for Dialed Number with EnterpriseName %1
CICR Replication found that a Dialed Number exists with this Enterprise Name. Therefore it cannot insert the new Dialed Number. CICR Replication cannot complete the replication in this case.			No action is required.
118C037	Single-state Raise	Warning	Duplicate Key Exists for Dialed Number with RoutingClientID %1 and DialedNumberString %2
CICR Replication found that a Dialed Number exists with this RoutingClientID and DialedNumberString. Therefore it cannot insert the new Dialed Number. CICR Replication cannot complete the replication in this case.			No action is required.
118C038	Single-state Raise	Warning	Duplicate Key Exists for Label with RoutingClientID %1 and LabelString %2.
CICR Replication found that a Label exists with this RoutingClientID and LabelString. Therefore it cannot insert the new Label. CICR Replication cannot complete the replication in this case.			No action is required.
118C039	Clear	Informational	CICR Replication on Side%1 is now Active.
The CICR Replication Process is Active.			No action is required.
118C03A	Raise	Informational	CICR Replication on Side%1 is now Inactive.
The CICR Replication Process is Inactive.			No action is required.
118C03D	Single-state Raise	Error	INVALID Hostname is configured for %1 customer. Use Config ICM tool to re-configure the hostname for %1 customer.
Invalid hostname is configured for the customer.			Use the ConfigICR->ICR_NODE to change the hostname or system name and re-start the CICR replication process.
118C03E	Single-state Raise	Warning	CICR Replication FAILED to Update CICR instance %1 due to CommitUpdateCCTransaction failure. Unable to Replicate to Customer %1. Check and correct the errors.
CICR Replication FAILED to update the configuration change due to the error caused by the CommitUpdateCCTransaction failure.			No action is required.
118C040	Single-state Raise	Warning	Found %1 records with DateTime greater than current Central Controller Time %2 in %3 table. Check and correct the errors.
Found historical records with DateTime greater than current Central Controller Time. Delete the records that have date time greater than the current central controller time.			No action is required.

118C048	Raise	Informational	NICR Replication on Side%1 is now Inactive.	
The NICR Replication Process is Inactive.				No action is required.
118C049	Clear	Informational	NICR Replication on Side%1 is now Active.	
The NICR Replication Process is Active.				No action is required.
118C04F	Raise	Warning	HDS Running Behind: %1 is running behind its Logger %2 by %3 minutes.	
Historical Database Server replicates behind its Logger by the time period specified in the registry. The HDS running status must be checked and/or the performance of both HDS and Logger must be monitored. The alarm controlling parameters may need to be adjusted to satisfy the specific requirement.				Verify HDS is running correctly. Check the performance of both Logger and HDS. If the HDS was shut down purposely, the alarm controlling parameters must be adjusted on the Logger to avoid additional alarms.
118C051	Single-state Raise	Error	INVALID Hostname (%1) is configured for primary distributor for %2 customer. Use Config ICM tool to re-configure the primary distributor for %2 customer.	
Invalid primary distributor is configured for the customer, or the system cannot resolve the hostname for the named primary distributor for some reason.				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.
11F0032	Raise	Error	Failed to connect to Meridian Link server at node %1 port %2.	
The Meridian PIM failed to connect to the Meridian Link server at node %1 and port %2.				Check the configuration defining the connection to the Meridian Link.
11F0033	Raise	Error	Connection to Meridian Link server at node %1 port %2 broken.	
The Meridian PIM connection to the Meridian Link server at node %1 and port %2 was broken.				Check that the Meridian Link platform is up and running and on the network.
11F0034	Clear	Informational	Successfully connected to and registered with Meridian Link server at node %1 port %2.	
The Meridian PIM successfully connected to and registered with the Meridian Link server at node %1 and port %2.				No action is required.
1288002	Clear	Informational	SS7 link %1 in service.	
The specified SS7 link is now aligned and in service.				No action is required.
1288003	Raise	Error	SS7 link %1 out of service.	
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.				Contact the Support Center.
128800A	Raise	Error	SS7 linkset %1 unavailable.	
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the NIC and the adjacent signaling point to which the linkset connects.				Contact the Support Center.
128800B	Clear	Informational	SS7 linkset %1 available.	
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 is restored.				No action is required.
1288101	Clear	Informational	BTNIC Gateway ONLINE.	
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 automatically proceeds.				No action is required.

1288102	Raise	Error	BTNIC Gateway STOPPED. (%1)
The NIC Gateway 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.			This event can be caused by a transient problem that 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.
12A4001	Clear	Informational	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.
A system (%1), via process (%2), connected to the SDDSN server 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.			No action is required.
12A4002	Raise	Error	SDDSN Unregistration was never received from system: %1, process: %2, using unique ID: %3. The registered system abruptly disconnected from the SDDSN server.
A system (%1), via process (%2), connected to the SDDSN server failed to unregistered as a valid endpoint using the unique ID (%3). This indicates that the system abruptly disconnected from the SDDSN server.			This could indicate that the SDDSN server 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 successfully re-registered the system(%1). This is indicated by a CLEAR condition to this alarm while the side of SDDSN that is reporting is 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 somehow failed.
12A4003	Clear	Informational	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.
A system (%1), via process (%2), connected to the SDDSN server successfully unregistered as a valid endpoint using the unique ID (%3). This indicates that the system gracefully disconnected from the SDDSN server.			No action is required.
12A400A	Single-state Raise	Error	The SDDSN server is missing, or has outdated, resource files and cannot decipher messages for product %1, (%3). Message ID = %2
An event is received that the SDDSN server cannot decipher using the resource files (message DLLs) because they are missing or out of date. The SDDSN server 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.			The SDDSN server must 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 product name. Install the updated support files for that product on the SDDSN server and restart it. This update contains files named MSGSn.DLL and CATn.DLL where the 'n' should be replaced with the number %1 from this error message (for example, MSGS2.DLL, CAT2.DLL, and so on.).
12A4010	Single-state Raise	Error	The client system: %3, attempted to send an incompatible version %1 SDDSN event. The current version supported is %2.

An event is received by a client system using an incompatible version of the SDDSN protocol.				To send the correct version of the SDDSN protocol, you must configure the client system. To support the desired version, you must upgrade the SDDSN server.
12B001F	Clear	Error	Application Gateway has connected with the host. Application Gateway ID = %1	
The application gateway is now connected to the host process.				No action is required.
12B0020	Raise	Error	The external database has disconnected from the Application Gateway (ID = %1). Routing may be impacted.	
An external database used in some Scripts disconnected from the specified Application Gateway. Error recovery mechanisms attempt to reconnect. Routing may be impacted.				Support group for external database should be contacted. If host database was off line for an extended period, re-starting the Application Gateway process may be necessary to re-connect.
12C8200	Clear	Informational	Communications to CICR %1 is ONLINE.	
At least one link with this CICR is now open and carrying traffic.				No action is required.
12C8201	Raise	Error	Communications to CICR %1 is OFFLINE.	
For some reason all the links to the CICR have terminated or were never established. If any links were established, there should be messages describing when and why the link or links failed. If configured to do so the CIC continues to attempt to open the links.				Determine why communications is not being established, which may include LAN or WAN configuration or the CICR machine failing.
12C8202	Clear	Informational	Link to CICR %1 side %2 is now ONLINE.	
A session with this CICR's side is now open and carrying traffic.				No action is required.
12C8203	Raise	Error	Link to CICR %1 side %2 is OFFLINE.	
For some reason the link to the CICR terminated or was never established. There is usually an error message preceding this message in the log file that gives an explanation for the link going down. If configured to do so the CIC will continue to attempt to open the link.				Determine why the link is not being established, which may include LAN or WAN configuration.
12C8204	Clear	Informational	Configuration for Link to CICR %1 side %2 is now VALID.	
The configuration for the connection between the Network ICM and the CICR's side is now valid.				No action is required.
12C8205	Raise	Error	Configuration for Link to CICR %1 side %2 is VOID.	
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 cannot keep multiple copies of the configuration and produces this error. If the latter problem occurs, simply reconfigure the link or links after they close.				Check the IP Address, Instance Number, and Preferred Side in the ICM Configuration for the Customer ICM and update the central data base.
12C8206	Clear	Informational	Link from CIC Side A to CICR %1 Side %2 is now ONLINE.	
A session with this CICR's side is now open and carrying traffic.				No action is required.
12C8207	Raise	Error	Link from CIC Side A to CICR %1 Side %2 is OFFLINE.	
For some reason the link to the CICR terminated or was never established. There is usually an error message preceding this message in the log file that gives an explanation for the link going down. If configured to do so the CIC continues to attempt to open the link.				Determine why the link is not being established, which may include LAN or WAN configuration.
12C8208	Clear	Informational	Configuration for Link between CIC Side A and CICR %1 Side %2 is now VALID.	
The configuration for the connection between the Network ICM and the CICR's side is				No action is required.

now valid.				
12C8209	Raise	Error	Configuration for Link between CIC Side A and CICR %1 Side %2 is VOID.	
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 cannot 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.				Check the IP Address, Instance Number, and Preferred Side in the ICM Configuration for the Customer ICM and update the central data base.
12C8210	Clear	Informational	Link from CIC Side B to CICR %1 Side %2 is now ONLINE.	
A session with this CICR's side is now open and carrying traffic.				No action is required.
12C8211	Raise	Error	Link from CIC Side B to CICR %1 Side %2 is OFFLINE.	
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 continues to attempt to open the link.				Determine why the link is not being established, which may include LAN or WAN configuration.
12C8212	Clear	Informational	Configuration for Link between CIC Side B and CICR %1 Side %2 is now VALID.	
The configuration for the connection between the Network ICM and the CICR's side is now valid.				No action is required.
12C8213	Raise	Error	Configuration for Link between CIC Side B and CICR %1 Side %2 is VOID.	
The configuration for the connection between the network Unified 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 cannot keep multiple copies of the configuration and produces this error. If the latter problem occurs, simply reconfigure the link or links after they have had time to close.				Check the IP Address, Instance Number, and Preferred Side in the ICM Configuration for the Customer ICM and update the central data base.
12D800A	Clear	Informational	Network ICM %1 is now accessible.	
The ICRP NIC established its first communication session with the indicated network Unified ICM. This indicates that network connectivity exists to the indicated NICR.				No action is required.
12D800B	Raise	Error	Network ICM %1 is no longer accessible.	
The ICRP NIC no longer has any communication sessions established with the indicated network Unified ICM. This points to a problem with the indicated NICR, or a problem with network connectivity.				ICRP Network support should be contacted regarding this problem.
12E8006	Clear	Informational	CONNECTION MONITOR SERVICE: Enterprise CTI session established by Client %1 (%2) at %3.	
An Enterprise CTI session was opened by ClientID %1 (Signature %2) from IP address %3.				No action is required.
12E8007	Raise	Warning	CONNECTION MONITOR SERVICE: Enterprise CTI session closed by Client %1 (%2) at %3.	
The Enterprise CTI session with ClientID %1 (Signature %2) at IP address %3 was closed by the client.				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.
12E8008	Raise	Error	CONNECTION MONITOR SERVICE: Enterprise CTI session terminated with Client %1 (%2) at %3.	

The Enterprise CTI session with ClientID %1 (Signature %2) at IP address %3 was terminated by the Enterprise CTI Server.				This indicates that an Enterprise CTI Client application that is normally always connected to the Enterprise CTI Server was disconnected due to errors. If the problem persists, the CTI Client application software may need to be checked for proper operation.
12E800C	Clear	Informational	Client:%1 Object:%2 Normal Event Report: %3	
The Enterprise CTI client %1 application software reported the following normal event for object %2: %3.				No action is required.
12E800D	Raise	Warning	Client:%1 Object:%2 Warning Event Report: %3	
The Enterprise CTI client %1 application software reported the following warning for object %2: %3.				This indicates that the CTI Client application software detected a possible error or other abnormal condition and may need to be checked for proper operation.
12E800E	Raise	Error	Client:%1 Object:%2 Error Event Report: %3	
The Enterprise CTI client %1 application software reported the following error for object %2: %3.				This indicates that the CTI Client application software detected an error condition and may need to be checked for proper operation.
12E800F	Raise	Warning	A Version 13 or prior CTI ClientID %1 (%2) at %3 connected with Agent multi line ENABLED.	
A CTI Client %1 (Signature %2) from IP address %3 with a version before 14 connected to CTI-Server that supports multi-line phones. Problems may be encountered with that application depending upon what messages/devices. it processes events for.				Check with the vendor of the software and see if they ensure compatability.
12E8010	Clear	Warning	A Version 13 or prior CTI ClientID %1 (%2) at %3 disconnected with Agent multi line ENABLED.	
A CTI Client %1 (Signature %2) from IP address %3 with a version before 14 connected to CTI-Server that supports multi-line phones. Problems may be encountered with that application depending upon what messages/devices it processes events for.				Check with the vendor of the software and see if they ensure compatability.
12F8009	Clear	Informational	SCP [%1:%2] is now accessible.	
The NORTEL NIC established a communication session with the indicated SCP. This indicates that network connectivity exists to the indicated SCP.				No action is required.
12F800A	Raise	Error	SCP [%1:%2] is no longer accessible.	
The NORTEL NIC disconnected the communication sessions established with the indicated SCP.				Nortel network support should be contacted regarding this problem.
12F800C	Clear	Informational	SCP [%1:%2] Accessible But Session to Other Side SCP[%1:%3] is still Active.	
The NORTEL NIC 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 occurred.				Determine cause of Failover.
12F8200	Clear	Informational	NTGATE ONLINE.	
The NORTEL NIC is online and is prepared to accept route requests from the Nortel network.				No action is required.
12F8201	Raise	Error	NTGATE OFFLINE.	
The NORTEL NIC is offline and cannot accept route requests from the Nortel network.				No action is required.
1338009	Raise	Error	StentorGate OFFLINE.	
The Stentor NIC is offline and cannot accept route requests from the Stentor network.				No action is required.
133800A	Clear	Informational	StentorGate ONLINE.	

The Stentor NIC is online and is prepared to accept route requests from the Stentor network.				No action is required.
133800B	Raise	Error	%1: Gateway is not in service or not reachable.	
The Stentor NIC either cannot establish or has lost communication with the indicated ATfG.				Stentor network support should be contacted regarding this problem.
133800C	Clear	Informational	%1: Connection established.	
The Stentor NIC established a communication session with the indicated ATfG. This indicates that network connectivity exists to the indicated ATfG.				No action is required.
1340017	Raise	Error	Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.	
INAP NIC cannot connect to the GATEWAY on the INAP network.				Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity allows for connection.
1348009	Clear	Informational	GATEWAY [%1] is now accessible.	
The INAP NIC established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.				No action is required.
134800A	Raise	Error	GATEWAY [%1] is no longer accessible.	
The INAP NIC disconnected the communication sessions established with the indicated GATEWAY.				Contact INAP network support regarding this problem.
134800C	Raise	Error	GATEWAY [%1] is not accessible.	
Although connected, the INAP NIC cannot establish a session with the indicated GATEWAY.				INAP network support should be contacted regarding this problem.
1348200	Clear	Informational	INAPGATE ONLINE.	
The INAP NIC is online and is prepared to accept route requests from the INAP network.				No action is required.
1348201	Raise	Error	INAPGATE OFFLINE.	
The INAP NIC is offline and cannot accept route requests from the INAP network.				No action is required.
1358004	Raise	Error	INRCEngine (DeviceID=%1) Initiating Admission Control.	
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.				If there is a problem in the Router, it may be a transient problem that clears without intervention. If 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.
1358005	Clear	Informational	INRCEngine (DeviceID=%1) Terminating Admission Control.	
The backlog of calls that caused Admission Control to be initiated was reduced to an acceptable level. Normal call routing resumed.				No action is required.
135800A	Raise	Warning	INRCEngine (DeviceID=%1) Initiating Restriction Control for CalledParty '%2'.	
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.				No action is required.
135800B	Clear	Informational	INRCEngine (DeviceID=%1) Terminating Restriction Control on CalledParty '%2'.	
Routing Client Engine is no longer restricting calls with the indicated called party number prefix.				No action is required.
1368002	Clear	Informational	SS7 link %1 in service.	
The specified SS7 link is now aligned and in service.				No action is required.

1368003	Raise	Error	SS7 link %1 out of service.	
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.				Contact the Support Center.
136800A	Raise	Error	SS7 linkset %1 unavailable.	
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the INAP Gateway and the adjacent signaling point to which the linkset connects.				Contact the Support Center.
136800B	Clear	Informational	SS7 linkset %1 available.	
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 was restored.				No action is required.
1368014	Clear	Informational	SS7 link %1 of linkset %2 is in service.	
The specified SS7 link is now aligned and in service.				No action is required.
1368015	Raise	Error	SS7 link %1 of linkset %2 is out of service.	
The specified SS7 link is now out of service. A circuit problem exists 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.				Contact the Support Center.
1368101	Clear	Informational	INAP Gateway ONLINE.	
The INAP Gateway has entered the online state. Traffic flow between the NIC and the SS7 network is enabled.				No action is required.
1368102	Raise	Error	INAP Gateway STOPPED. (%1)	
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 adminstrative 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, alert the Support Center to investigate and correct the problem.
138800A	Clear	Informational	Network ICM %1 is now accessible.	
The INCRP NIC established its first communication session with the indicated Network Unified ICM. This indicates that network connectivity exists to the indicated NICR.				No action is required.
138800B	Raise	Error	Network ICM %1 is no longer accessible.	
The INCRP NIC no longer has any communication sessions established with the indicated Network Unified ICM. This points to a problem with the indicated NICR, or a problem with network connectivity.				Contact INCRP Network support regarding this problem.
139800A	Clear	Informational	Network ICM %1 is now accessible.	
The NEC NIC has established its first communication session with the indicated SCP. This indicates that network connectivity exists to the indicated SCP.				No action is required.
139800B	Raise	Error	Network ICM %1 is no longer accessible.	
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.				Contact NEC Network support regarding this problem.

13A8202	Clear	Informational	Dialogue on SVC %1 is now OPEN.	
A dialog with the SCP is now open and available to carry traffic.				No action is required.
13A8203	Raise	Error	Dialogue on SVC %1 is now CLOSED.	
The NIC has an existing SVC open to the SCP and is waiting for a dialog open message. The NIC waited for a configured amount of time and has not received a dialog open message.				Determine if the SCP application is running and sending open requests.
13A8206	Clear	Informational	FTGATE ONLINE.	
The France Telecom NIC is online and is prepared to accept route requests from the network.				No action is required.
13A8207	Raise	Error	FTGATE OFFLINE.	
The France Telecom NIC is offline and cannot accept route requests from the network.				No action is required.
13E0003	Raise	Error	Message Integration Service (MIS) was unable to connect to %1%2 on %3 TCP/IP Port %4.	
Message Integration Service cannot connect to the indicated component and address.				Confirm Component is available, Configuration of IP addresses and Ports are correct, and Network connectivity allows for connection
13E0004	Clear	Informational	Connection to %1%2 on Address[%3:%4] Succeeded.	
Message Integration Service can connect to the indicated component and address.				No action is required.
13E0005	Raise	Error	Message Integration Service (MIS) was unable to open a session to %1%2.	
Message Integration Service cannot open a session to the indicated component				No action is required.
13E0006	Clear	Informational	Session to %1%2 Opened.	
Message Integration Service can open a session to the indicated component and address.				No action is required.
13E0007	Single-state Raise	Error	TrunkGroup:%1 Trunk:%2 Received in Msg from Vru-%3 Not Configured	
A message pertaining to the indicated trunk group and trunk was not configured with MIS				Configure Extension, Trunk Group, and Trunk in MIS.
13E0008	Single-state Raise	Error	Call Tracking Error: %1	
A call within MIS cannot be tracked successfully.				Determine where tracking problem occurred and correct (for MIS problem could be MIS, VRU, or PG).
13F8200	Clear	Informational	Session with Client Id %1 SCP index %2 configuration valid.	
If a configuration error occurred, it is cleared when the session is closed.				No action is required.
13F8201	Raise	Error	Session with Client Id %1 SCP index %2 configuration invalid.	
A problem 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 that was not configured in the open session message.				Determine if the SCP is on line and if the communications links are available.
13F8202	Clear	Informational	Session with Client Id %1 SCP index %2 is now OPEN.	
A session with the SCP is now open and available to carry traffic.				No action is required.
13F8203	Raise	Error	Session with Client Id %1 SCP index %2 is now CLOSED.	
No session is currently opened with the SCP. The SCP index indicates the relative position of the configuration for that SCP in the NT Registry.				Determine if the SCP is on line and if the communications links are available.
13F8206	Clear	Informational	CRSP GATE ONLINE.	

The CRSP NIC is online and is prepared to accept route requests from the network.				No action is required.
13F8207	Raise	Error	CRSP GATE OFFLINE.	
The CRSP NIC is offline and cannot accept route requests from the network.				No action is required.
1420017	Raise	Error	Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.	
CWC NIC cannot connect to the GATEWAY on the CWC network.				Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity allows for connection.
1428009	Clear	Informational	GATEWAY [%1] is now accessible.	
The CWC NIC established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.				No action is required.
142800A	Raise	Error	GATEWAY [%1] is no longer accessible.	
The CWC NIC disconnected the communication sessions established with the indicated GATEWAY.				Contact CWC network support regarding this problem.
142800C	Raise	Error	GATEWAY [%1] is not accessible.	
Although connected, the CWC NIC cannot establish a session with the indicated GATEWAY.				Contact CWC network support regarding this problem.
1428200	Clear	Informational	C&W NIC Routing Client is ONLINE.	
The CWC NIC is online and is prepared to accept route requests from the CWC network.				No action is required.
1428201	Raise	Error	C&W NIC Routing Client is OFFLINE.	
The CWC NIC is offline and cannot accept route requests from the CWC network.				No action is required.
1428203	Clear	Informational	SS7 link %1 in service.	
The specified SS7 link is now aligned and in service.				No action is required.
1428204	Raise	Error	SS7 link %1 out of service.	
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.				Contact the Support Center.
142820B	Raise	Error	SS7 linkset %1 unavailable.	
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the INAP Gateway and the adjacent signaling point to which the linkset connects.				Contact the Support Center.
142820C	Clear	Informational	SS7 linkset %1 available.	
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 is restored.				No action is required.
1428210	Clear	Informational	INAP Gateway ONLINE.	
The INAP Gateway entered the online state. Traffic flow between the NIC and the SS7 network is enabled.				No action is required.
1428211	Raise	Error	INAP Gateway STOPPED. (%1)	
The INAP Gateway 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,				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,

or by an adminstrative INAP Gateway command.				the Support Center should be alerted to investigate and correct the problem.
1428310	Raise	Error	SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).	
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.				No action is required.
1428311	Clear	Informational	SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).	
The specified SS7 link is now aligned and in service.				No action is required.
1428312	Raise	Error	SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).	
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the SS7 Gateway and the adjacent signaling point to which the linkset connects.				Contact the Support Center.
1428313	Clear	Informational	SS7 linkset available (Gateway PC=%1, Linkset RPC=%2).	
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 is restored.				No action is required.
1438000	Raise	Error	Blended Agent Campaign Manager on [%1] is down.	
The Blended Agent Campaign Manager is not running. Dialers only run for a short period of time without a Campaign Manager. In addition, configuration messages cannot be forwarded to Dialers or the Import process.				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 be created with the ICMDBA tool.
1438001	Clear	Informational	Blended Agent Campaign Manager on [%1] is up.	
Blended Agent Campaign Manager is ready to distribute customer records and configuration data.				No action is required.
1438002	Single-state Raise	Error	Failed to execute import into table [%1] due to a change in the tables' schema.	
The schema for a specified table was changed but the overwrite option was not enabled. This means that an existing database table does not match the configured import.				Change the import to an overwrite import. This drops the existing customer table and creates a new table that matches the import. All existing customer data for that import is lost.
1438003	Single-state Raise	Error	Import failed due to an invalid table [%1] definition.	
Could not create the specified table due to invalid import schema definition.				Check that all table columns for the failed import are correct. Making a character column too long could cause this failure.
1438004	Clear	Informational	The import for table [%1] has been successful.	
An import has completed successfully.				No action is required.
1438005	Single-state Raise	Error	Failed to import data into table [%1].	
This error could occur if the import file did not match the table definition.				Check that the import table definition matches the import file.

1438006	Single-state Raise	Error	Failed to build dialing list from table [%1].
A Dialing list could not be populated from the specified table.			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.
1438007	Single-state Raise	Error	Could not open [%1] database.
The Blended Agent private database was initialized or SQL Server is not running.			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?
1438008	Single-state Raise	Error	An import was started but its configuration was deleted while it was running.
An import started running but part of its configuration was deleted before it can do anything.			Reschedule the import.
1438009	Raise	Error	Blended Agent CTI Server connection on computer [%1] is down.
The Blended Agent CTI Server connection was terminated.			Make sure CTI Server is active. Also make sure the PIM has connectivity to the switch.
1438010	Clear	Informational	Blended Agent CTI Server connection on computer [%1] is active.
Blended Agent CTI Server connection is active.			No action is required.
1438011	Raise	Error	Dialer telephony port [%1] is not functioning correctly.
A telephony error occured 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 be disconnected or cut.			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 telepohony card 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.
1438012	Clear	Informational	Blended Agent telephony port [%1] has recovered.
A previously malfunctioning telephony port has received a message from the telephony driver indicating the ports is back in service.			No action is required.
1438013	Raise	Error	BAImport is down on the computer [%1].
BAImport is not running on the specified computer.			Ensure that the Import process was not shutdown. Check that the BA Private database was created. Also, check that SQL Server is running.
1438014	Clear	Informational	BAImport is up on the computer [%1].
BAImport is running on the specified computer.			No action is required.
1438015	Raise	Error	Dialer is down on the computer [%1].
Dialer is down on the specified computer.			Ensure that the Dialogic drivers are configured and running. Also verify that the Dialer is started by Node Manager.
1438016	Clear	Informational	Dialer is up on the computer [%1].

Dialer is up on the specified computer.				No action is required.
1438019	Single-state Raise	Error	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.	
Failed to rename or delete the import file for Import Rule Id: <id; filename>. This Import Rule is temporarily disabled. To correct this condition: manually remove the import file and disable and re-enable the import rule using Import Configuration Component.				File polling is enabled for this import rule. After the import, the BAImport process cannot 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.
1438020	Single-state Raise	Error	Campaign [%1] trying to [%2] and database timed out.	
Campaign <campaign name> tried to run a query <query name> and database timed out.				No action is required.
1438021	Single-state Raise	Error	Database is running out of space.	
Database is running out of space.				Create some space in the database.
1438022	Single-state Raise	Error	The Agent SkillGroup [%1] recieved is not the configured SkillGroup [%2] for the Campaign [%3].	
The Agent skill group recieved is not configured for this campaign.				Make sure the skill group configured in the script is the same as the skill group configured in the campaign.
1438023	Single-state Raise	Warning	Timeout happening for the call on Port [%1]. Time to get the MR response : [%2 seconds].	
Timeout happening for the call on port.				Timeout happening for a call on Port. Check the Registry Key TimeToWaitForMRIResponse.
1438024	Raise	Error	Media Routing PIM Disconnected with the Dialer [%1].	
Media Routing PIM Disconnected with the Dialer.				Check whether the MR PIM is active or not.
1438025	Clear	Error	MR PIM connected to Dialer [%1].	
MR PIM connected to Dialer <dialer name>.				No action is required.
1438026	Single-state Raise	Error	Import ID [%1] has more than 10000 Errors.	
Import Process has more than 10000 errors.				Restart the Import Process.
1438027	Single-state Raise	Error	Dialer [%1] with incorrect protocol version trying to connect.	
Dialer with incorrect protocol version trying to connect.				Check the Dialer version.
1438028	Single-state Raise	Error	Campaign [%1] DNC list to be imported has exceeded the total number of DNC Records allowed. Check the CampaignManager log files for more details.	
The DNC List to be imported has exceeded the number of DNC Records set by ConfigLimit				Check the DNC record limit set by the ConfigLimit tool.
1438029	Single-	Error	For %1 process System Out Of Memory.	

	state Raise		
Memory overflow. Cannot instantiate or assign enough memory.			This is a memory outage, and the configuration of the system may not be sufficient.
1438030	Single-state Raise	Error	Dialer: Unknown Port Owner [%1]
Dialer: Unknown Port Owner.			Check the Administrator scripts.
1438031	Single-state Raise	Error	Cannot find key [%1] in the Registry.
Cannot find key in the Registry.			Ensure that the installation process went smooth.
1438032	Single-state Raise	Error	Unable to open Registry key: [%1]
Unable to open Registry key.			Ensure that the installation process went smooth.
1438033	Single-state Raise	Error	Campaign Manager could not connect to the BA private Database.
Campaign Manager could not connect to the BA private Database.			Make sure the SQL Server is running and the Blended Agent private database is initialized.
1438034	Single-state Raise	Error	Dialer attempted to connect to incorrect Campaign Manager version [%1], required version [%2]
Dialer attempted to connect to incorrect Campaign Manager version.			Ensure that the Campaign Manager is compatible with the Dialer Version.
1438035	Single-state Raise	Error	Your configured Dialer type [%1] does not match this Dialer type [%2]
Configured Dialer type does not match this Dialer type.			Check the Dialer type configured. IP or SIP.
1438036	Single-state Raise	Error	Dialer has too many ports configured [%1], maximum allowed [%2]
Dialer has too many ports configured.			Decrease the number of Ports configured.
1438037	Single-state Raise	Error	Campaign Manager: Unable to convert System Time to FileTime
Campaign Manager: Cannot convert System Time to FileTime			No action is required.
1438038	Raise	Error	Blended Agent connection to SIP Server [%1] on computer [%2] is down, heart beat failure detected
Blended Agent SIP Server heart beat failure, the connection is down.			Ensure SIP Server is alive and reachable from Blended Agent SIP Dialer.
1438040	Single-state Raise	Error	Current private database version is [%1]. Required version is [%2].
Blended Agent private database version is not correct. It needs to be upgraded using EDMT.			Upgrade private database to the correct version using EDMT for this release.
1438041	Single-	Error	Missing\incorrect local Static Route File is detected on [%1] in the

	state Raise		directory, ..\icm\[%2]\Dialer.].
Static route file, ..\Dialer\DNPHost, is missing or has no valid static route entry when configuring the SIP Dialer to connect to voice Gateway.			Re-run the Dialer setup to install smaple DNPHost file, and/or enter valid static route entry.
1438042	Single-state Raise	Error	CPA is disabled on voice gateway [%1],Number of calls without CPA: [%2].
CPA is disabled or not supported on voice gateway.			Enable CPA on voice gateway.
1438043	Single-state Raise	Error	Action Required : BA Db Space Availability Remaining is very less: [%1%%]
BA Database Space Utilization reached the Threshold Limit.			Increase the DB space utilization or remove unnecesary records from the BA Database.
1438044	Clear	Informational	[%1] has insufficient records [%2] in the last one minute on the Dialer machine [%3]
Campaign skill group has insufficient customer records.			Increase the 'records to cache' from the Campaign configuration.
1438045	Single-state Raise	Warning	Voice Gateway has been overdialed in the last [%1] seconds. Resource Not Available Rate is %2%%, Configured-Current Port Throttle: [%3].
The capacity of Voice Gateway or Carrier was exceeded.			Check the capacity of Voice Gateway or Carrier, and adjust the value of 'Port Throttle' from the Dialer Configuaration accordingly.
1438046	Single-state Raise	Warning	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].
SIP Dialer decreases the port throttle because the capacity of Voice Gateway or Carrier is exceeded.			Adjust the value of 'Port Throttle' from the Dialer configuration or check BOM to do proper sizing calculation for Outbound Dialer.
1440017	Raise	Error	Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.
ENERGIS NIC cannot connect to the GATEWAY on the ENERGIS network.			Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity allows for connection
1448009	Clear	Informational	GATEWAY [%1] is now accessible.
The ENERGIS NIC established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.			No action is required.
144800A	Raise	Error	GATEWAY [%1] is no longer accessible.
The ENERGIS NIC disconnected the communication sessions established with the indicated GATEWAY.			Contact ENERGIS network support regarding this problem.
144800C	Raise	Error	GATEWAY [%1] is not accessible.
Although connected, the ENERGIS NIC cannot establish a session with the indicated GATEWAY.			Contact ENERGIS network support regarding this problem.
1448012	Clear	Informational	SS7 link %1 in service.
The specified SS7 link is now aligned and in service.			No action is required.

1448013	Raise	Error	SS7 link %1 out of service.	
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.				Contact the Support Center.
144801A	Raise	Error	SS7 linkset %1 unavailable.	
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the INAP Gateway and the adjacent signaling point to which the linkset connects.				Contact the Support Center.
144801B	Clear	Informational	SS7 linkset %1 available.	
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 is restored.				No action is required.
1448101	Clear	Informational	INAP Gateway ONLINE.	
The INAP Gateway entered the online state. Traffic flow between the NIC and the SS7 network is enabled.				No action is required.
1448102	Raise	Error	INAP Gateway STOPPED. (%1)	
The INAP Gateway 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 adminstrative 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.
1448200	Clear	Informational	ENERGISGATE ONLINE.	
The ENERGIS NIC is online and is prepared to accept route requests from the ENERGIS network.				No action is required.
1448201	Raise	Error	ENERGISGATE OFFLINE.	
The ENERGIS NIC is offline and cannot accept route requests from the ENERGIS network.				No action is required.
1450017	Raise	Error	Session for Gateway[%1] Connect FAILED to Gateway at Port %2 at Address %3.	
CAIN NIC cannot connect to the Gateway on the CAIN network.				Confirm Gateway is available, configuration of IP address and Port are correct, and network connectivity allows for connection.
1458009	Clear	Informational	Gateway[%1] is now accessible (GSP open response accepted).	
The CAIN NIC established a communication session with the indicated Gateway. This indicates that network connectivity exists to the indicated Gateway.				No action is required.
145800A	Raise	Error	Gateway[%1] is no longer accessible (GSP session closed).	
The CAIN NIC disconnected the communication sessions established with the indicated Gateway.				CAIN network support should be contacted regarding this problem.
145800C	Raise	Error	Gateway[%1] not accessible (no GSP open response returned); retrying...	
Although connected, the CAIN NIC cannot establish a session				CAIN network support should be contacted

with the indicated Gateway.			regarding this problem.	
1458200	Clear	Informational	CAINGATE is now ONLINE.	
The CAIN NIC is online and is prepared to accept route requests from the CAIN network.				No action is required.
1458201	Raise	Error	CAINGATE is now OFFLINE.	
The CAIN NIC is offline and cannot accept route requests from the CAIN network.				No action is required.
1458301	Clear	Informational	SS7 link %1 of linkset %2 is in service.	
The specified SS7 link is now aligned and in service.				No action is required.
1458302	Raise	Error	SS7 link %1 of linkset %2 is out of service.	
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.				Contact the Support Center.
1458309	Raise	Error	SS7 linkset %1 unavailable.	
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the AIN Gateway and the adjacent signaling point to which the linkset connects.				Contact the Support Center.
145830A	Clear	Informational	SS7 linkset %1 available.	
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 is restored.				No action is required.
1458400	Clear	Informational	AIN Gateway ONLINE.	
The AIN Gateway entered the online state. Traffic flow between the NIC and the SS7 network is enabled.				No action is required.
1458401	Raise	Error	AIN Gateway STOPPED. (%1)	
The AIN Gateway 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 adminstrative AIN Gateway command.			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.	
1460017	Raise	Error	Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.	
Unisource NIC cannot connect to the GATEWAY on the Unisource network.			Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity allows for connection	
1468009	Clear	Informational	GATEWAY [%1] is now accessible.	
The Unisource NIC established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.				No action is required.

146800A	Raise	Error	GATEWAY [%1] is no longer accessible.	
The Unisource NIC disconnected the communication sessions established with the indicated GATEWAY.				Contact Unisource network support regarding this problem.
146800B	Raise	Error	GATEWAY [%1] is not accessible.	
Although connected, the Unisource NIC cannot establish a session with the indicated GATEWAY.				Contact Unisource network support regarding this problem.
146800D	Clear	Informational	SS7 link %1 in service.	
The specified SS7 link is now aligned and in service.				No action is required.
146800E	Raise	Error	SS7 link %1 out of service.	
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.				Contact the Support Center.
1468015	Raise	Error	SS7 linkset %1 unavailable.	
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the SS7 Gateway and the adjacent signaling point to which the linkset connects.				Contact the Support Center.
1468016	Clear	Informational	SS7 linkset %1 available.	
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 is restored.				No action is required.
1468017	Clear	Informational	SS7 Gateway ONLINE.	
The SS7 Gateway entered the online state. Traffic flow between the NIC and the SS7 network is enabled.				No action is required.
1468018	Raise	Error	SS7 Gateway STOPPED. (%1)	
The SS7 Gateway 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 adminstrative SS7 Gateway command.				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.
1468200	Clear	Informational	UNISOURCE Routing Client is ONLINE.	
The Unisource NIC is online and is prepared to accept route requests from the Unisource network.				No action is required.
1468201	Raise	Error	UNISOURCE Routing Client is OFFLINE.	
The Unisource NIC is offline and cannot accept route requests from the Unisource network.				No action is required.
1468310	Raise	Error	SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).	
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				No action is required.

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.				
1468311	Clear	Informational	SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).	
The specified SS7 link is now aligned and in service.				No action is required.
1468312	Raise	Error	SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).	
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the SS7 Gateway and the adjacent signaling point to which the linkset connects.				Contact the Support Center.
1468313	Clear	Informational	SS7 linkset available (Gateway PC=%1, Linkset RPC=%2).	
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 is restored.				No action is required.
1468314	Raise	Error	SCTP connection is down (ConnectionNumber = %1, Remote Entity = %2).	
The SCTP Association to the remote entity is down. Communication failed and calls cannot be processed through this connection. Check the Gateway logs for configuration errors and/or check the remote entity.				No action is required.
1468315	Raise	Error	ASP is Down (ConnectionNumber = %1, Remote Entity = %2).	
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.				No action is required.
1468316	Raise	Error	ASP is Inactive (ConnectionNumber = %1, Remote Entity = %2).	
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.				No action is required.
1468317	Clear	Informational	ASP is Active (ConnectionNumber = %1, Remote Entity = %2).	
The ASP is Active. Calls can be processed through this connection.				No action is required.
1490017	Raise	Error	Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.	
CONCERT NIC cannot connect to the GATEWAY on the CONCERT network.				Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity allows for connection
1498009	Clear	Informational	GATEWAY [%1] is now accessible.	
The CONCERT NIC established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.				No action is required.
149800A	Raise	Error	GATEWAY [%1] is no longer accessible.	
The CONCERT NIC disconnected the communication sessions established with the indicated GATEWAY.				CONCERT network support should be contacted regarding this problem.
149800C	Raise	Error	GATEWAY [%1] is not accessible.	
Although connected, the CONCERT NIC cannot establish a session with the indicated GATEWAY.				CONCERT network support should be contacted regarding this problem.
1498200	Clear	Informational	CONCERTGATE ONLINE.	

The CONCERT NIC is online and is prepared to accept route requests from the CONCERT network.				No action is required.
1498201	Raise	Error	CONCERTGATE OFFLINE.	
The CONCERT NIC is offline and cannot accept route requests from the CONCERT network.				No action is required.
1498203	Clear	Informational	SS7 link %1 in service.	
The specified SS7 link is now aligned and in service.				No action is required.
1498204	Raise	Error	SS7 link %1 out of service.	
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.				Contact the Support Center.
149820B	Raise	Error	SS7 linkset %1 unavailable.	
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the INAP Gateway and the adjacent signaling point to which the linkset connects.				Contact the Support Center.
149820C	Clear	Informational	SS7 linkset %1 available.	
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 is restored.				No action is required.
1498210	Clear	Informational	INAP Gateway ONLINE.	
The INAP Gateway entered the online state. Traffic flow between the NIC and the SS7 network is enabled.				No action is required.
1498211	Raise	Error	INAP Gateway STOPPED. (%1)	
The INAP Gateway 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 adminstrative 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.
14A0002	Raise	Error	Connection to %1%2 on Address[%3:%4] failed.	
MEI Server cannot connect to the indicated Meridian MAX.				Confirm Meridian MAX is available, Configuration of IP addresses and Ports are correct, and Network connectivity allows for connection
14A0003	Clear	Informational	Connection to %1%2 on Address[%3:%4] Succeeded.	
MEI Server can connect to the indicated Meridian MAX.				No action is required.
14A0004	Raise	Error	Session to %1%2 Not Open	
MEI Server cannot open a session to the indicated Meridian MAX				Confirm Meridian MAX is available and configured correctly.
14A0005	Clear	Informational	Session to %1%2 Opened.	
MEI Server can open a session to the indicated Meridian MAX.				No action is required.

14B0017	Raise	Error	Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.
TELFORT NIC cannot connect to the GATEWAY on the TELFORT network.			Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity allows for connection
14B8009	Clear	Informational	GATEWAY [%1] is now accessible.
The TELFORT NIC established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.			No action is required.
14B800A	Raise	Error	GATEWAY [%1] is no longer accessible.
The TELFORT NIC disconnected the communication sessions established with the indicated GATEWAY.			Contact TELFORT network support regarding this problem.
14B800C	Raise	Error	GATEWAY [%1] is not accessible.
Although connected, the TELFORT NIC cannot establish a session with the indicated GATEWAY.			Contact TELFORT network support regarding this problem.
14B8200	Clear	Informational	TELFORT NIC Routing Client is ONLINE.
The TELFORT NIC is online and is prepared to accept route requests from the TELFORT network.			No action is required.
14B8201	Raise	Error	TELFORT NIC Routing Client is OFFLINE.
The TELFORT NIC is offline and cannot accept route requests from the TELFORT network.			No action is required.
14B8203	Clear	Informational	SS7 link %1 in service.
The specified SS7 link is now aligned and in service.			No action is required.
14B8204	Raise	Error	SS7 link %1 out of service.
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.			Contact the Support Center.
14B820B	Raise	Error	SS7 linkset %1 unavailable.
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the INAP Gateway and the adjacent signaling point to which the linkset connects.			Contact the Support Center.
14B820C	Clear	Informational	SS7 linkset %1 available.
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 is restored.			No action is required.
14B8210	Clear	Informational	INAP Gateway ONLINE.
The INAP Gateway entered the online state. Traffic flow between the NIC and the SS7 network is enabled.			No action is required.
14B8211	Raise	Error	INAP Gateway STOPPED. (%1)
The INAP Gateway 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			This event can be caused by a transient problem, which may be automatically corrected as indicated by a 'INAP Gateway online' event.

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 adminstrative INAP Gateway command.				If the problem persists for more than three minutes, the Support Center should be alerted to investigate and correct the problem.
14B8310	Raise	Error	SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).	
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.				No action is required.
14B8311	Clear	Informational	SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).	
The specified SS7 link is now aligned and in service.				No action is required.
14B8312	Raise	Error	SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).	
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the SS7 Gateway and the adjacent signaling point to which the linkset connects.				Contact the Support Center.
14B8313	Clear	Informational	SS7 linkset available (Gateway PC=%1, Linkset RPC=%2).	
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 is restored.				No action is required.
14C0017	Raise	Error	Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2 at Address %3.	
BT-V2 INAP NIC cannot connect to the GATEWAY on the INAP network.				Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity allows for connection
14C8009	Clear	Informational	GATEWAY [%1] is now accessible.	
The BT-V2 INAP NIC established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.				No action is required.
14C800A	Raise	Error	GATEWAY [%1] is no longer accessible.	
The BT-V2 INAP NIC disconnected the communication sessions established with the indicated GATEWAY.				INAP network support should be contacted regarding this problem.
14C800C	Raise	Error	GATEWAY [%1] is not accessible.	
Although connected, the BT-V2 INAP NIC cannot establish a session with the indicated GATEWAY.				INAP network support should be contacted regarding this problem.
14C8200	Clear	Informational	BT-V2 NIC Routing Client is ONLINE.	
The BT-V2 INAP NIC is online and is prepared to accept route requests from the INAP network.				No action is required.
14C8201	Raise	Error	BT-V2 NIC Routing Client is OFFLINE.	
The BT-V2 INAP NIC is offline and cannot accept route requests from the INAP network.				No action is required.
14C8203	Clear	Informational	SS7 link %1 in service.	

The specified SS7 link is now aligned and in service.				No action is required.
14C8204	Raise	Error	SS7 link %1 out of service.	
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.				Contact the Support Center.
14C820B	Raise	Error	SS7 linkset %1 unavailable.	
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the INAP Gateway and the adjacent signaling point to which the linkset connects.				Contact the Support Center.
14C820C	Clear	Informational	SS7 linkset %1 available.	
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 is restored.				No action is required.
14C8210	Clear	Informational	INAP Gateway ONLINE.	
The INAP Gateway entered the online state. Traffic flow between the NIC and the SS7 network is enabled.				No action is required.
14C8211	Raise	Error	INAP Gateway STOPPED. (%1)	
The INAP Gateway 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 adminstrative 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.
14C8310	Raise	Error	SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).	
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.				No action is required.
14C8311	Clear	Informational	SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).	
The specified SS7 link is now aligned and in service.				No action is required.
14C8312	Raise	Error	SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).	
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the SS7 Gateway and the adjacent signaling point to which the linkset connects.				Contact the Support Center.
14C8313	Clear	Informational	SS7 linkset available (Gateway PC=%1, Linkset RPC=%2).	
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 is restored.				No action is required.
14D0017	Raise	Error	Session for GATEWAY[%1] Connect FAILED to GATEWAY at Port %2	

			at Address %3.
TIM NIC cannot connect to the GATEWAY on the INAP network.			Confirm GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity allows for connection
14D8009	Clear	Informational	GATEWAY [%1] is now accessible.
The TIM NIC established a communication session with the indicated GATEWAY. This indicates that network connectivity exists to the indicated GATEWAY.			No action is required.
14D800A	Raise	Error	GATEWAY [%1] is no longer accessible.
The TIM NIC disconnected the communication sessions established with the indicated GATEWAY.			Contact INAP network support regarding this problem.
14D800C	Raise	Error	GATEWAY [%1] is not accessible.
Although connected, the TIM NIC cannot establish a session with the indicated GATEWAY.			Contact INAP network support regarding this problem.
14D8200	Clear	Informational	TIM NIC Routing Client is ONLINE.
The TIM NIC is online and is prepared to accept route requests from the INAP network.			No action is required.
14D8201	Raise	Error	TIM NIC Routing Client is OFFLINE.
The TIM NIC is offline and cannot accept route requests from the INAP network.			No action is required.
14D8203	Clear	Informational	SS7 link %1 in service.
The specified SS7 link is now aligned and in service.			No action is required.
14D8204	Raise	Error	SS7 link %1 out of service.
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.			Contact the Support Center.
14D820B	Raise	Error	SS7 linkset %1 unavailable.
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the INAP Gateway and the adjacent signaling point to which the linkset connects.			Contact the Support Center.
14D820C	Clear	Informational	SS7 linkset %1 available.
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 is restored.			No action is required.
14D8210	Clear	Informational	INAP Gateway ONLINE.
The INAP Gateway entered the online state. Traffic flow between the NIC and the SS7 network is enabled.			No action is required.
14D8211	Raise	Error	INAP Gateway STOPPED. (%1)
The INAP Gateway 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 adminstrative 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.
14D8310	Raise	Error	SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.			No action is required.
14D8311	Clear	Informational	SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).
The specified SS7 link is now aligned and in service.			No action is required.
14D8312	Raise	Error	SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the SS7 Gateway and the adjacent signaling point to which the linkset connects.			Contact the Support Center.
14D8313	Clear	Informational	SS7 linkset available (Gateway PC=%1, Linkset RPC=%2).
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 is restored.			No action is required.
14D8314	Raise	Error	SCTP connection is down (ConnectionNumber = %1, Remote Entity = %2).
The SCTP Association to the remote entity is down. Communication failed and calls cannot be processed through this connection. Check the Gateway logs for configuration errors and/or check the remote entity.			No action is required.
14D8315	Raise	Error	ASP is Down (ConnectionNumber = %1, Remote Entity = %2).
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.			No action is required.
14D8316	Raise	Error	ASP is Inactive (ConnectionNumber = %1, Remote Entity = %2).
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.			No action is required.
14D8317	Clear	Informational	ASP is Active (ConnectionNumber = %1, Remote Entity = %2).
The ASP is Active. Calls can be processed through this connection.			No action is required.
14E0008	Raise	Warning	Session [%1] closed for reason '%2' by client '%3'.
The client terminated a communication session with the GKTMP NIC.			No action is required.
14E0009	Clear	Informational	Session for Client[%1] status[%2] connected to Client %3.
GKTMP NIC Successfully established a connection with the client.			No action is required.
14E0013	Clear	Informational	GKTMP NIC ONLINE.
The GKTMP NIC is online and is prepared to accept route requests from its clients.			No action is required.
14E0014	Raise	Error	GKTMPGATE OFFLINE.
The GKTMP NIC is offline and cannot accept route requests from clients.			No action is required.
14F0017	Raise	Error	Session for GATEWAY[%1] Connect FAILED to SS7 GATEWAY at Port

			%2 at Address %3.
SS7 IN NIC cannot connect to the SS7 GATEWAY.			Confirm SS7 GATEWAY is available, Configuration of IP address and Port are correct, and Network connectivity allows for connection
14F8009	Clear	Informational	SS7 GATEWAY [%1] is now accessible.
The SS7 IN NIC established a communication session with the indicated SS7 GATEWAY. This indicates that network connectivity exists to the indicated SS7 GATEWAY.			No action is required.
14F800A	Raise	Error	SS7 GATEWAY [%1] is no longer accessible.
The SS7 IN NIC disconnected the communication sessions established with the indicated SS7 GATEWAY.			SS7 network support should be contacted regarding this problem.
14F800C	Raise	Error	SS7 GATEWAY [%1] is not accessible.
Although connected, the SS7 IN NIC cannot establish a session with the indicated GATEWAY.			SS7 network support should be contacted regarding this problem.
14F8102	Clear	Informational	SS7 link %1 in service.
The specified SS7 link is now aligned and in service.			No action is required.
14F8103	Raise	Error	SS7 link %1 out of service.
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.			Contact the Support Center.
14F810A	Raise	Error	SS7 linkset %1 unavailable.
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the SS7 Gateway and the adjacent signaling point to which the linkset connects.			Contact the Support Center.
14F810B	Clear	Informational	SS7 linkset %1 available.
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 is restored.			No action is required.
14F8114	Clear	Informational	SS7 link %1 of linkset %2 is in service.
The specified SS7 link is now aligned and in service.			No action is required.
14F8115	Raise	Error	SS7 link %1 of linkset %2 is out of service.
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.			Contact the Support Center.
14F8310	Raise	Error	SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).
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			No action is required.

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 failed. If this occurs, a 'linkset unavailable' alarm is generated.				
14F8311	Clear	Informational	SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).	
The specified SS7 link is now aligned and in service.				No action is required.
14F8312	Raise	Error	SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).	
The specified SS7 linkset is now unavailable. This means that no links in that linkset are operational. Consequently, communication failed between the SS7 Gateway and the adjacent signaling point to which the linkset connects.				Contact the Support Center.
14F8313	Clear	Informational	SS7 linkset available (Gateway PC=%1, Linkset RPC=%2).	
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 is restored.				No action is required.
14F8314	Raise	Error	SCTP connection is down (ConnectionNumber = %1, Remote Entity = %2).	
The SCTP Association to the remote entity is down. Communication failed and calls cannot be processed through this connection. Check the Gateway logs for configuration errors and/or check the remote entity.				No action is required.
14F8315	Raise	Error	ASP is Down (ConnectionNumber = %1, Remote Entity = %2).	
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.				No action is required.
14F8316	Raise	Error	ASP is Inactive (ConnectionNumber = %1, Remote Entity = %2).	
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.				No action is required.
14F8317	Clear	Informational	ASP is Active (ConnectionNumber = %1, Remote Entity = %2).	
The ASP is Active. Calls can be processed through this connection.				No action is required.
1504001	Application Error	Error	The NTL NIC received an invalid label %1 from the Router for the call(tid=%2).	
The NTL NIC received an invalid label from the Router. Check the label format and size.				Check labels in the label table for invalid labels.
1508006	Clear	Informational	Starting NTL network communications.	
The network communication layer of the NTL NIC is starting operation.				No action is required.
1508007	Raise	Warning	Stopping NTL network communications.	
The network communication layer of the NTL NIC is halting operation.				No action is required.
1508009	Clear	Informational	Starting a NTL communication channel (%1) with CE '%4:%2'.	
A communication channel of the NTL NIC is starting operation.				No action is required.
150800A	Raise	Error	Stopping the NTL communication channel (%1) to CE '%4:%2'.	
A communication channel of the NTL NIC is halting operation.				No action is required.
150800B	Raise	Error	Closing the NTL communication channel (%1) by CE '%4:%2'.	
A communication channel of the NTL NIC is closed by the SCP.				No action is required.

1520017	Raise	Error	Session for Gateway[%1] Connect FAILED to Gateway at Port %2 at Address %3.
NIC cannot connect to the Gateway on the SS7 network.			Confirm Gateway is available, configuration of IP address and Port are correct, and network connectivity allows for connection.
1528009	Clear	Informational	Gateway[%1] is now accessible (GSP open response accepted).
The NIC established a communication session with the indicated Gateway. This indicates that network connectivity exists to the indicated Gateway.			No action is required.
152800A	Raise	Error	Gateway[%1] is no longer accessible (GSP session closed).
The NIC disconnected the communication sessions established with the indicated Gateway.			SS7 network support should be contacted regarding this problem.
152800C	Raise	Error	Gateway[%1] not accessible (no GSP open response returned); retrying...
Although connected, the NIC cannot establish a session with the indicated Gateway.			SS7 network support should be contacted regarding this problem.
1528200	Clear	Informational	AT&T Routing Client is ONLINE.
The NIC is online and is prepared to accept route requests from the SS7 network.			No action is required.
1528201	Raise	Error	AT&T Routing Client is OFFLINE.
The NIC is offline and cannot accept route requests from the SS7 network.			No action is required.
1528301	Clear	Informational	SS7 link %1 of linkset %2 is in service.
The specified SS7 link is now aligned and in service.			No action is required.
1528302	Raise	Error	SS7 link %1 of linkset %2 is out of service.
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 failed. If this occurs, a 'linkset unavailable' alarm is generated.			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&T Advanced Features Service Center (AFSC) at 800-621-6901. Ask to speak to an ICP technician.
1528309	Raise	Error	SS7 linkset %1 unavailable.
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. Because the network interface utilizes two linksets, each connected to a different STP, network connectivity is not impacted unless both linksets failed.			Occasional brief outages of a single link (and hence a single linkset) are not unusual and require no action. If the outage persists for more than five minutes, or if the outage occurs frequently, contact the AT&T Advanced Features Services Center (AFDSC) at 800-621-6901. Ask to speak to an ICP technician.
152830A	Clear	Informational	SS7 linkset %1 available.
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 is restored.			No action is required.
1528310	Raise	Error	SS7 Link is out of service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3) (%4).

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 failed. If this occurs, a 'linkset unavailable' alarm is generated.				No action is required.
1528311	Clear	Informational	SS7 Link is in service (Gateway PC=%1, Linkset RPC=%2, Link SLC=%3).	
The specified SS7 link is now aligned and in service.				No action is required.
1528312	Raise	Error	SS7 linkset unavailable (Gateway PC=%1, Linkset RPC=%2).	
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. Because the network interface utilizes two linksets, each connected to a different STP, network connectivity is not impacted unless both linksets failed.				Occasional brief outages of a single link (and hence a single linkset) are not unusual and require no action. If the outage persists for more than five minutes, or if the outage occurs frequently, contact the AT&T Advanced Features Services Center (AFDSC) at 800-621-6901. Ask to speak to an ICP technician.
1528313	Clear	Informational	SS7 linkset available (Gateway PC=%1, Linkset RPC=%2).	
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 is restored.				No action is required.
1528314	Raise	Error	SCTP connection is down (ConnectionNumber = %1, Remote Entity = %2).	
The SCTP Association to the remote entity is down. Communication failed and calls cannot be processed through this connection. Check the Gateway logs for configuration errors or check the remote entity.				No action is required.
1528315	Raise	Error	ASP is Down (ConnectionNumber = %1, Remote Entity = %2).	
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.				No action is required.
1528316	Raise	Error	ASP is Inactive (ConnectionNumber = %1, Remote Entity = %2).	
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.				No action is required.
1528317	Clear	Informational	ASP is Active (ConnectionNumber = %1, Remote Entity = %2).	
The ASP is Active. Calls can be processed through this connection.				No action is required.
1528400	Clear	Informational	SS7 Gateway ONLINE.	
The SS7 Gateway entered the online state. Traffic flow between the NIC and the SS7 network is enabled.				No action is required.
1528401	Raise	Error	SS7 Gateway STOPPED. (%1)	
The SS7 Gateway 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				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

NIC, by a problem with the Router, or by an adminstrative SS7 Gateway command.			investigate and correct the problem.
1530002	Raise	Error	A required parameter is invalid.
One or more of the required parameters are invalid.			Internal error. Contact tech support.
1530003	Raise	Error	The maximum SEI event queue size was exceeded.
The maximum SEI event queue size was exceeded.			Change the configuration in the registry (for more information, see Troubleshooting Guide) to allow for a greater queue size.
1530015	Raise	Error	One or more ICM/AW connection parameters are null or empty.
One or more required Unified ICM/AW connection parameters are null or empty.			Ensure that all required Unified ICM/AW connection information exists in the registry and is correct (for more information, see Troubleshooting Guide). If the information is in the registry and is correct, contact technical support.
1530017	Raise	Error	Fatal connection error to ICM/AW.
All retry and failover attempts to the Unified ICM AW failed.			For information about correcting connection errors, see the AAS Installation and Troubleshooting Guide.
1530018	Raise	Error	ICM/AW authentication failed.
AAS cannot log into the Unified ICM/AW because the login authentication failed.			Check sign-in information in the registry (for more information, see Troubleshooting Guide) and make sure it matches the sign-in information used to setup the application on the ICM/AW.
1530019	Raise	Error	Unable to retrieve a PG Name from the Peripheral table.
Unable to retrieve a PG Name from the Peripheral table.			Make sure a PG Name is configured for the peripheral that is set up for AAS.
153001A	Raise	Error	Error adding record to ICM/AW.
AAS cannot add a record to the Unified ICM/AW. A possible reason is that the Unified ICM/AW is out of sync with Symposium.			Resync Unified ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (for more information, see Troubleshooting Guide).
153001B	Raise	Error	Error deleting record from ICM/AW.
AAS cannot delete a record from Unified ICM/AW. A possible reason is that the Unified ICM/AW is out of sync with Symposium.			Resync Unified ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (for more information, see Troubleshooting Guide).
153001C	Raise	Error	Error updating record in ICM/AW.
AAS cannot update a record in Unified ICM/AW. A possible reason is that the Unified ICM/AW is out of sync with Symposium.			Resync Unified ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (for more information, see Troubleshooting Guide).
153001D	Raise	Error	Error performing bulk update of the ICM/AW.
AAS cannot perform a bulk update of the Unified ICM/AW. A possible reason is that the Unified ICM/AW is out of sync with Symposium.			Resync Unified ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (for more information, see Troubleshooting Guide).
153001E	Raise	Error	Bad ICM/AW operation type used.
A bad Unified ICM/AW operation type was used. Update, delete, insert, and destroy permanently are the only operation types supported.			Internal error. Contact technical support.
153001F	Raise	Error	Lost connection to the ICM/AW.

AAS lost its connection to the Unified ICM/AW due to an unknown cause.			AAS should self-correct. If it does not, consult the AAS Installation and Troubleshooting Guide for information about correcting connection errors to Unified ICM.
1530020	Raise	Error	Error retrieving records from the ICM/AW.
AAS cannot retrieve records from the Unified ICM/AW. A possible reason is that the Unified ICM/AW is out of sync with Symposium.			Resync Unified ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (for more information, see Troubleshooting Guide).
1530021	Raise	Error	Error retrieving peripheral record from ICM/AW.
AAS cannot retrieve a peripheral record from Unified ICM/AW. The record was not created in the Unified ICM/AW or the ID for it was not set properly in the registry.			Make sure a peripheral is set up in the Unified ICM/AW for AAS. Ensure the peripheral ID is properly configured in the AAS configuration registry (for more information, see Troubleshooting Guide).
1530022	Raise	Error	Error retrieving skill group from ICM/AW.
AAS cannot retrieve a skill group from Unified ICM/AW. A possible reason is that the Unified ICM/AW is out of sync with Symposium.			Resync Unified ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (for more information, see Troubleshooting Guide).
1530023	Raise	Error	Agent priority specified is beyond maximum allowed limits.
The agent priority specified was configured with a priority greater than the maximum allowed limit of 48.			Internal error. Contact technical support.
1530025	Raise	Error	An attempt was made to remove an agent from a skill group and either the agent or the skill group does not exist.
AAS attempted to remove an agent from a skill group and either the agent or the skill group does not exist.			Resync Unified ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (for more information, see Troubleshooting Guide).
1530026	Raise	Error	An attempt was made to remove an agent from a skill group where no such assignment exists.
An attempt was made to remove an agent from a skill group where no such assignment exists.			Resync Unified ICM/AW with Symposium by incrementing the value of AASForceResync in the registry (for more information, see Troubleshooting Guide).
1530027	Raise	Error	A request was made to add an agent in a bulk operation where no corresponding person exists.
A request was made to add an agent in a bulk operation where no corresponding person exists.			No action is required.
1530033	Raise	Error	Config services requested before config info set.
Configuration services were requested before the configuration information was set up.			Internal error. Contact technical support.
1530034	Raise	Error	An unexpected key type was given to the config service.
A configuration parameter for AAS was configured with the wrong key type in the registry.			Recreate the key with the proper type (for more information, see Troubleshooting Guide).
1530035	Raise	Error	All attempts to connect to Symposium have failed.
All attempts to connect to Symposium failed.			Ensure that all the Symposium services are started and running. Check that the Symposium configuration/connection information is correct.
1530036	Raise	Error	Error performing post resync processing.
There was an error while performing post-resync processing.			Check for a broken connection to the Unified ICM

The error occurred during Unified ICM/AW processing while trying to cache data from the Unified ICM database.			or other errors in the log for problems accessing the database.
1530037	Raise	Error	An event was discarded.
An event was discarded due to a data access exception received from Unified ICM/AW (ConAPI).			No action is required.
1530038	Raise	Error	Registration with SEI server failed.
The registration with SEI server failed.			Ensure the SEI configuration in the registry (for more information, see Troubleshooting Guide) is correct.
1530039	Raise	Error	Request for initial SEI events failed.
The request for initial SEI events failed.			Make sure the Symposium services are started and functioning properly.
1530040	Raise	Error	AAS failed to establish a connection to SEI.
AAS failed to establish a connection to SEI.			No action is required.
1530041	Raise	Error	The maximum allowable event queue size has been exceeded.
The maximum allowable event queue size was exceeded even though the Unified ICM/AW appears to be functioning normally. Some causes are a slow network, a slow Unified ICM/AW, or a slow database.			The problem may be fixed by increasing the value in the AASSEIMaxEventQueueSize registry (for more information, see Troubleshooting Guide) setting.
1530051	Raise	Error	Configuration given to MasterSelection is null.
MasterSelection cannot start because the AAS PG hosts and ports were not configured in the registry.			Correct registry data for AASPG Hosts and Ports (for more information, see Troubleshooting Guide).
1530052	Raise	Error	Bad IP address for Side A MasterSelection.
The configuration IP address for the Side A MasterSelection is badly formed or cannot be found.			Correct the AASPGHostA and AASPGPortA configuration data in the registry (for more information, see Troubleshooting Guide).
1530053	Raise	Error	Bad IP address for Side B MasterSelection.
The configuration IP address for the Side B MasterSelection is badly formed or cannot be found.			Correct the AASPGHostB and AASPGPortB configuration data in the registry (for more information, see Troubleshooting Guide).
1530054	Raise	Error	Null IP address for Side A MasterSelection.
The configuration IP address for the Side A MasterSelection is blank, which is not allowed.			Correct the AASPGHostA and AASPGPortA configuration data in the registry (for more information, see Troubleshooting Guide).
1530055	Raise	Error	Null IP address for Side B MasterSelection.
The configuration IP address for the Side B MasterSelection is blank, which is not allowed.			Correct the AASPGHostB and AASPGPortB configuration data in the registry (for more information, see Troubleshooting Guide).
1530056	Raise	Error	BindException or SocketException trying to open socket for MasterSelection.
MasterSelection could not open a socket for communication.			The network administrator should make sure the Side A and B servers can communicate with each other.
1530057	Raise	Error	Due to the max event queue size being exceeded, a resync of Symposium events is being requested.
A Symposium resync is being requested because the maximum event queue size was exceeded.			This is most likely due to a configuration error in the registry. Check the registry (for more information, see Troubleshooting Guide) and make sure it is correct.

15301F4	Raise	Informational	AAS disconnected from the ICM/AW.	
AAS disconnected from the Unified ICM/AW.			AAS should reset its connection to Unified ICM. If it does not, restart AAS.	
15301F6	Clear	Informational	Connection to the ICM/AW established.	
The connection between AAS and the Unified ICM/AW has been established.			No action is required.	
1530235	Clear	Informational	MasterSelection has been started.	
MasterSelection IP addresses were checked, a socket opened, and threads started.			No action is required.	
1540002	Single-state Raise	Error	An error occurred on the TCP/IP connection between the ACMI ACD Server (CTI) and the ACMI peripheral gateway. ACMI peripheral gateway is offline.	
An error occurred on the connection between the ACMI ACD Server(CTI) and the ACMI peripheral gateway. ACMI peripheral gateway is offline.			If ACMI peripheral gateway does not re-attach contact the Support Center.	
1540003	Clear	Informational	Peripheral status was DOWN, going NORMAL. ACMI peripheral gateway is online.	
Peripheral status was DOWN, going NORMAL. ACMI peripheral gateway is online.			No action is required.	
1540007	Clear	Informational	The route register on the DN %1 is Operational.	
The DN is Operational.			No action is required.	
1540008	Raise	Error	The route register failed for DN %1.	
The Permit Application Routing box on the child system is not checked for DN.			Check Permit Application Routing box.	
1540009	Raise	Error	The route register failed for DN %1.	
You configured a DN or DN for a translation route on the parent that does not exist on the child system – do not forget to check 'Permit Application Routing' when adding it.			Add the DN on child system and ensure that Permit Application Routing is enabled.	
154000A	Raise	Error	The route register failed for DN %1.	
You configured a DN or DN for a translation route on the parent that does not exist on the child system – do not forget to check 'Permit Application Routing' when adding it.			Add the DN on child system and ensure that Permit Application Routing is enabled.	
154000B	The route register failed for DN %1.	Error	The route register failed for DN %1.	
You specified an incorrect Server Peripheral ID in the PG Setup of the Gateway PG.			Correct the Server Peripheral ID in the PG Setup of the Gateway PG and cycle the PG.	
154000C	Single-state Raise	Error	The route register failed for DN %1.	
Another Gateway PG requested control of this DN - likely incorrect Server hostname configured.			Correct the Server hostname in the PG Setup of the Gateway PG and cycle the PG.	
154000D	Single-state Raise	Error	The peripheral id %1 given is not valid.	
You specified an incorrect Server Peripheral ID in the PG Setup of the Gateway PG.			Correct the Server Peripheral ID in the PG Setup of the Gateway PG and cycle the PG.	

154000E	Single-state Raise	Error	Central Controller Connection on Child Down - ACMI peripheral gateway status DOWN.
Central Controller Connection on Child Down - ACMI peripheral gateway status DOWN.			No action is required.
1560004	Clear	Informational	CTI OS Server version %2 is online. Connected to CTI Server at %3. CTI Server protocol is %1.
Message indicating the version of CTI OS Server as well as the protocol version CTI OS Server uses to connect to CTI Server.			No action is required.
1560005	Raise	Warning	CTI OS Server version %2 cycled because the connection to CTI Server at %3 closed. CTI Server protocol is %1.
CTI OS Server cycled itself because its connection to CTI Server closed. When CTI OS Server restarts, it re-establishes its connection to CTI Server.			This event usually occurs when the CTI Server process cycles. If this event is received and CTI Server was not manually cycled, collect the CTI OS Server log as well as all PG logs and contact Cisco customer support.
1560006	Raise	Error	CTI OS Server version %2 cycled because the connection to CTI Server at %3 failed. CTI Server protocol is %1.
CTI OS Server cycled itself because its connection to CTI Server failed. When CTI OS Server restarts, it re-establishes its connection to CTI Server.			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, 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%, check the agent, team, and skill group configuration with the SRND to make sure it is within tolerance.
1560007	Clear	Informational	CTI OS Server has %1 messages in Queue.
The CTI OS Server incoming message is now below 10000 messages.			No action is required.
1560008	Raise	Warning	CTI OS Server has %1 messages in Queue.
The CTI OS Server incoming message queue exceeded 10000 messages. This might result in unwanted behavior.			This event can occur when CTI OS is running on a heavily loaded system. If this event is received, 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%, check the agent, team, and skill group configuration with the SRND to make sure it is within tolerance.
1560009	Raise	Error	CTI OS Server has generated an exception in %2 processing a %3.\n Details:\n %4: %1\n %5
CTI OS Server generated an exception while processing a request or an event specified in this method.			This is an internal error with the CTI OS Server request and message processing logic. Collect the CTI OS Server log and all PG logs and contact Cisco customer support.
156000A	Raise	Error	CTI OS Server has generated an exception in %2 processing %3.\n Details:\n %4: %1\n %5
CTI OS Server generated an exception while processing the request or event specified in this method.			This is an internal error with the CTI OS Server request and message processing logic. Collect the CTI OS Server log and all PG logs and contact Cisco customer support.
156000B	Clear	Informational	The CTI OS Server total amount of agent mode connections is %1. This is within the CTI OS Server limit of %2.
CTI OS Server is current running with an acceptable number of agents connected to it.			No action is required.
156000C	Clear	Warning	The CTI OS Server total amount of agent mode connections is %1. This exceeds the CTI OS Server limit of %2.
CTI OS Server is currently running with an excessive number of agents			Ensure that the number of agents currently using the system is not more than the limit listed in the event description. If there are custom CTI OS

connected to it.			applications deployed in the contact center, make sure to understand how many connections those custom applications open to the CTI OS Server. For example, if a custom application opens two connections to CTI OS Server, only half the number of agents can connect to the CTI OS Server.
156000D	Clear	Informational	The CTI OS Server total amount of monitor mode connections is %1. This is within the CTI OS Server limit of %2.
CTI OS Server is current running with an acceptable number of monitor-mode applications connected to it.			No action is required.
156000E	Clear	Warning	The CTI OS Server total amount of monitor mode connections is %1. This exceeds the CTI OS Server limit of %2.
CTI OS Server is currently running with an excessive number of monitor-mode applications connected to it.			Ensure that the number of monitor mode applications connected to the CTI OS Server does not exceed the limit listed in the event 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 the CTI OS Server as well as what types of connections those applications open to the CTI OS Server. For example, applications that appear to open an agent mode connection (presents a UI geared toward an agent) may also open a monitor mode connection in the background.
156000F	Clear	Informational	The CTI OS Server monitor mode functionality has been re-enabled. Monitor mode functionality was previously disabled after %1 failed attempts to access monitor mode functionality.
CTI OS Server has re-enabled monitor mode functionality.			No action is required.
1560010	Raise	Warning	CTI OS Server monitor mode functionality has been disabled after %1 failed attempts to access monitor mode functionality.
CTI OS Server 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.			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 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 unlocks after the configured amount of time (15 minutes by default).
12A0003	n/a	n/a	HeartBeat Event for %1
Periodic message to indicate MDS is in service and that the event stream is active.			No action is required.