Release Notes for *Cisco IPCC/ICM Enterprise & Hosted Editions Release 7.0(0) Installer Update C*

November 24, 2008

Updated Information in this Document

This document updates the October 03, 2007 version with the following changes:

Section and Page	Notes	Date Added
Accessing Schema Help from ICM Master Help On a Limited AW (CSCsv77964), page 82	Describes how to resolve the error message that results from attempting to access Schema online help from the ICM Master Help on a Limited AW.	24Nov2008
Clarification on Some Agent_Skill_Group_Half_Hour and Skill_Group_Half_Hour Fields, page 71	Provides clarifying information regarding a number of fields in the two tables mentioned.	3Oct2008
Network Consultative Transfer Limited to 3-party Conference, page 71	Describes how NCT can be used for conferences.	3Jul2008
CallsAnsweredToHalf Does Not Include InternalCallsReceivedToHalf, page 71	The field CallsAnsweredToHalf includes only inbound calls, not internal calls.	21May2008
ICM-to-ICM Gateway User Guide, page 72	Points out that the section “Configuring ICM Instances on the Client ICM” should be ignored.	10Apr2008
Configuration Parameters for Routing Client on INCRP NIC, page 72	Discusses the equivalence of the /ssn switch and the /CustomerID switch.	10Apr2008
Obsolete NICs Removed, page 33	Additional information is provided regarding obsoleted NICs.	5Apr2008
Time Zone and Daylight Savings Time Updates, page 75	Discusses how to keep current with worldwide changes in time zones and on what date daylight savings time occurs.	21Mar2008

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Section and Page	Notes	Date Added
CallManager 4.x Consideration for External Calls in IPCC Enterprise, page 75	Discusses an issue where overlap sending is disabled by default in the CallManager 4.x gateway configuration.	21Mar2008
Manual Intervention to Restart ICM Processes after an Exception, page 76	Describes how to avoid manual intervention when restarting an ICM Process after an exception.	23Jan2008
Remote Desktop Not Supported for Installation, page 76	Remote Desktop must not be used for installation.	15Jan2008
Dynamic Agent Re-Skilling, page 16	Clarifies that supervisors can only perform changes on agents they supervise.	15Jan2008
User Variable Name Restriction, page 76	As of Release 7.0(0), periods/dots (.) are not allowed in User Variable names.	9Jan2008
Average Speed of Answer (ASA) Report Calculation, page 78	Corrected discussion of the registry value DeliveredEventsResetASACalculation.	4Jan2008
Replicating Configuration Changes from NAM to CICM & NAM to NAM, page 77	Discusses this topic in light of Active Directory.	28Dec2007
Security Best Practices Guide and Windows OS Support, page 71	For the currently supported Windows operating system software, see the latest *Hardware and System Software Specification (Bill of Materials) for Cisco ICM/IPCC Enterprise and Hosted Editions*, not the *Security Best Practices Guide*.	16Oct2007
Outbound Option: CallsMadeToZone, page 72	More explicitly indicates the value of CallsMadeToZone.	5Oct2007
Outbound Option: Call Marked Closed when Transfer to IVR/Agent on AMD, page 77	Discusses consequences of configuring transfer to an agent or IVR.	5Oct2007
Service Level and Services Auto-Configured in a Unified ICME Parent/Unified CCX Child Model, page 72	Discusses how to access Service Level information in a Unified ICME Parent/Unified CCX Child environment.	1Oct2007
WebView Real-Time Data and Peripheral Gateway (PG) Failover, page 77	Discusses what happens to WebView real-time data if a PG failover occurs.	1Oct2007

Contents

New IPCC/ICM 7.0(0) Installer Update C Discs

Cisco has issued new versions of a number of IPCC/ICM 7.0(0) discs to address defects found in IPCC/ICM 7.0(0) software, and improve Setup. These changes affect the following products:

- IPCC Enterprise & Hosted Editions 7.0(0)
- System IPCC Enterprise Edition 7.0(0)
- ICM Enterprise & Hosted Editions 7.0(0)

Note IPCC/ICM Version 7.0(0) Installer Update C fixes defects in the 7.0(0)B "media setup" files. The name “Installer Update” indicates that the "media setup" files have been updated to fix setup defects. In an Installer Update, *only* the "media setup" related files are modified. Cisco best practices require that you must install the most recent Service Releases (SRs) and Maintenance Releases (MRs) before bringing up the ICM services or running local setup. Specifically, to fix these same defects for IPCC/ICM "local setup", customers must apply MR 7.1(2) or a subsequent SR/MR. Contact the Cisco Technical Assistance Center (see Obtaining Technical Assistance, page 88) for more details.

About the IPCC/ICM 7.0(0) Installer Update C Discs

The new discs are labeled as follows:

- Cisco Unified Contact Center Enterprise Version 7.0(0) Installer Update C
- Cisco Unified Contact Center Hosted Version 7.0(0) Installer Update C
- Cisco Unified ICM Enterprise Version 7.0(0) Installer Update C
- Cisco Unified ICM Hosted Version 7.0(0) Installer Update C
- Cisco Unified System Contact Center Enterprise DVD Version 7.0(0) Installer Update C
- Cisco Unified Contact Center Products 3rd Party Tools Version 7.0(0) Installer Update C

Note The content of the 3rd Party Tools disc has not changed between V7.0(0)B and V7.0(0) Installer Update C. It has been relabeled simply for consistency. If you have already installed 3rd Party Tools from a V7.0(0)B disc, you need not reinstall.

With few exceptions, the defects resolved by IPCC/ICM 7.0(0) Installer Update C are relevant only at install or upgrade time. There is no need to immediately install IPCC/ICM 7.0(0) Installer Update C if you are already successfully running Release 7.0. However, in all cases (affected or not) you should replace your existing ICM software 7.0(0) discs with new ICM software 7.0(0) Installer Update C discs; this will help to prevent problems when the discs are used for future ICM upgrades or modifications to your installation.

Note Once you have installed Release 7.0(0) Installer Update C, check the registry key **[HKLM]\SOFTWARE\Cisco Systems, Inc.\ICM\SystemSettings\InstallUpdateVersion** The value of the key will be *7.0(0)_IU_C* where IU means Installer Update and C is the version of the Installer built on 7.0(0).

You can request new discs online:

https://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=421&fid=861

Note An updated version of the *Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* will be available on cisco.com. The updated guide can be recognized by an October, 2006 publication date on the cover page. Customers planning to install or upgrade to IPCC/ICM 7.0(0) are urged to read the updated Staging Guide before attempting to install or upgrade. This updated document contains new guidelines related to Active Directory. In particular, the updated Staging Guide warns that customers should use a single forest for the IPCC/ICM domain topology. Customers currently using multiple forests should migrate their IPCC/ICM servers to a single forest before deployment of 7.0(0), then continue use of this deployment with any future versions of ICM. Please refer to the updated Staging Guide for additional information.

Setup Change in IPCC/ICM 7.0(0) Installer Update C

Prior to IPCC/ICM 7.0(0) Installer Update C, the following could occur on a server running multiple IPCC instances, with multiple users having privileges on various instances.

A user, who did not have Setup rights on all the instances, could use Upgrade All. Upgrade All would then only upgrade the instances for which the user had setup permission.

However, when this happened, the icm\bin and registry would be updated. In instances for which the user did not have setup permission, files might get deleted, user registries might get updated, but service accounts would not be updated. This could leave these instances in a poorly defined state.

In IPCC/ICM 7.0(0) Installer Update C, when Upgrade All is used, Setup checks that the user has setup permission on *ALL* instances on the server. This check is done before any instances are upgraded. If the user has permission on all instances, then upgrade proceeds. Otherwise, Setup exits with a warning that the user has inadequate permission.

Defects Corrected in the New IPCC/ICM 7.0(0) Installer Update C Discs

The new IPCC/ICM 7.0(0) Installer Update C software corrects these defects:

Identifier	Component	Headline
CSCsc49512	aw.config.list	User List Tool and Agent Explorer tool are slow to display users
CSCse50977	aw.config.list	WebView favorite, private and scheduled reports lost w/ upgrade to 7.0
CSCsd59723	security	In multiple domain scenario user in config group cannot run config tools
CSCsd24683	setup	User w/ setup permissions can't add component after DomainManager closes
CSCsd44965	setup	Setup fails if user's primary group is changed to Domain Administrator
CSCsd93156	setup	Services fail to start due to login failures after setup finishes
CSCse00799	setup	Setup appears to hang while upgrading db if domain improperly configured
CSCse07066	setup	OPC crashes on the idle side of the PG
CSCse09940	setup	Domain Manager returns wrong domain/facility/instance values in setup.
CSCse54974	setup	User with setup permissions unable to run setup.
CSCse09424	setup.pg	Can't turn on MIS in ICM setup for VRU PG
CSCse15910	setup.pg	Local setup deletes registry keys added in 5.0SR13 ES6 (Definity PG only)
CSCse20906	setup.pim	Unable to Configure NEAX2400 PIM through ICM Setup
CSCse44161	setup.webview.ICM	ICM Setup fails to set Jaguar Service Account correctly

IPCC/ICM Software Release 7.0(0)B

Note If you have Release 7.0(0)B installed, and right-click on <drive>:\icm\bin\sadlib.dll and select Properties, there will be a Version tab with the version 1.0.0.1. If you have an earlier Release installed, there will be no version tab.

The IPCC/ICM 7.0(0)B software corrected the following defects:

Defect ID	Description
CSCsc32260	Install or Upgrade fails if external trusted domain is unavailable
CSCsc74727	Outbound dialer does not dial and imports fail after upgrading to 7.0
CSCsc99326	WebView 3rd party (EAServer 5.1) install/upg fails when pcAnywhere there
CSCsd20312	EDMT upgrade fails for databases originating prior to ICM/IPCC 4.6.2
CSCsd57079	Setup fails upgrading AW databases originating prior to ICM/IPCC 4.6.2
CSCsd59887	EDMT intermittently fails with "invalid object name" error

IPCC/ICM Software Release 7.0(0)A

Soon after the initial release of IPCC/ICM 7.0(0), the following defect was detected:

Defect ID	Description
CSCsb47495	SSL utility gives errors on Chinese and Korean W2003

No CDs containing the defect had gone to affected markets, so no Field Notice was issued. However, since the image on the CDs had changed, the updated CDs that resolved the defect were relabeled V7.0(0)A. IPCC/ICM 7.0(0) SR1 normalized all fielded 7.0 customers to 7.0(0)A status.

IPCC/ICM Software Release 7.0(0)

The rest of this document discusses the new features, technical changes, and so on that are associated with IPCC/ICM software Release 7.0(0).

New Enhanced Data Migration Tool (EDMT)

Cisco has issued a new version of EDMT to address defects found in the EDMT software. These defects affect upgrading to the following products:

- IPCC Enterprise & Hosted Editions 7.0(0)
- ICM Enterprise & Hosted Editions 7.0(0)

About the New EDMT

The Enhanced Database Migration Tool (EDMT) for ICM/IPCC 7.0 is no longer available as a CD. It must be downloaded from

http://www.cisco.com/kobayashi/sw-center/telephony/icm/icm-planner.shtml

Any references to the EDMT CD in the *Upgrade Guide for Cisco ICM/IPCC Enterprise & Hosted Editions: Release 7.0(0)* should be read with this in mind.

The defects resolved by the new version of EDMT 7.0(0) are relevant only at upgrade time. There is no need to immediately install the new version of EDMT if you are already successfully running Release 7.0. However, in all cases (affected or not) you should replace your existing EDMT software with the new EDMT software; this will help to prevent problems when EDMT is used for future ICM upgrades or modifications to your installation.

Defects Corrected by the New EDMT

The new EDMT software corrects these defects:

Defect ID	Description
CSCse27987	EDMT nulls some historical data columns moving from 6.0 to 7.0
CSCse21210	EDMT changing UserNames to all-caps may violate UNIQUE constraint

Details about these defects follow:

Defect ID: CSCse27987

Headline: EDMT nulls some historical data columns moving from 6.0 to 7.0

Symptom:
In the process of using EDMT to upgrade a database from ICM/IPCC 6.0 to 7.0B, the following columns are erased and set to NULL.

TABLE NAME: t_Call_Type_Half_Hour:

CallsAnsweredToHalf

CallsRoutedNonAgentToHalf

CallsRONAToHalf

ReturnReleaseToHalf
CallsQHandledToHalf
VruUnhandledCallsToHalf
VruHandledCallsToHalf
VruAssistedCallsToHalf
VruOptOutUnhandledCallsToHalf
VruScriptedXferredCallsToHalf
VruForcedXferredCallsToHalf
VruOtherCallsToHalf
ServiceLevelType
BucketIntervalID
AnsInterval1
AnsInterval2
AnsInterval3
AnsInterval4
AnsInterval5
AnsInterval6
AnsInterval7
AnsInterval8
AnsInterval9
AnsInterval10
AbandInterval1
AbandInterval2
AbandInterval3
AbandInterval4
AbandInterval5
AbandInterval6
AbandInterval7
AbandInterval8
AbandInterval9
AbandInterval10
DbDateTime

TABLE NAME: t_Route_Call_Detail:
DbDateTime
BeganRoutingDateTime
BeganCallTypeDateTime
TargetType

RequeryResult

VruProgress

TABLE NAME: t_Termination_Call_Detail:

DbDateTime

NetQTime

Conditions: EDMT upgrade from ICM/IPCC 6.0(0), 6.0(0)A or 6.0(0)B to 7.0B.

Defect ID: CSCse21210

Headline: EDMT changing UserNames to all-caps may violate UNIQUE constraint

Symptom:
EDMT fails during upgrade of an ICM/IPCC 5.0 or 6.0 database with the following errors:

User_Group: updateData: Violation of UNIQUE Key constraint 'XAK1User_Group'. Cannot insert duplicate key in object 'User_Group

User_Group_Member: updateData: Violation of UNIQUE Key constraint 'XAK1User_Group_Member'. Cannot insert duplicate key in object 'User_Group_Member

Conditions: System contains user names which become duplicates when converted to all upper-case. An example would be the user names "User1" and "USER1".

Introduction

IPCC/ICM software Release 7.0(0) supports:

- ICM Enterprise Edition
- ICM Hosted Edition
- IPCC Enterprise Edition
- IPCC Hosted Edition

This document discusses new features, changes, and caveats for Release 7.0(0) of IPCC/ICM Enterprise and Hosted software.

Note Cisco Web Collaboration Option 5.0 and Cisco E-Mail Manager Option 5.0 are supported by IPCC/ICM Release 7.0(0). However, Cisco Web Collaboration Option 5.0 and Cisco E-Mail Manager Option 5.0 are not supported with System IPCC Enterprise deployment, or the IPCC System PG, and therefore are not supported for the parent/child relationship established by the IPCC Enterprise Gateway PG.

Note **The Network Consultative Transfer (NCT) feature for IPCC/ICM Hosted Edition, though documented in the 7.0(0) Hosted manuals, will only become available in a subsequent Service Release.**

Additional information on new features, and on many of the product changes, is available in the relevant end-user documentation.

- Release Notes for Cisco CTI Object Server, Cisco Agent Desktop, Cisco E-Mail Manager Option, Cisco Web Collaboration Option (including Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender) are separate documents and are not included as part of these Release Notes.

Note For the most up-to-date version of these release notes, as well as all other ICM/ IPCC documentation, go to the Cisco Web page: http://www.cisco.com

System Requirements

For hardware and third-party software specifications for Release 7.0(0), refer to the *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)*, which is accessible from
http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm

Related Documentation

Documentation for Cisco IPCC/ICM Enterprise and Hosted Editions, as well as most related documentation, is accessible from
http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm

- Related documentation includes the documentation sets for Cisco CTI Object Server (CTI OS), Cisco Agent Desktop (CAD), Cisco E-Mail Manager Option, Cisco Web Collaboration Option (including Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender), Cisco Customer Voice Portal (CVP), Cisco IP IVR, Cisco Support Tools, and Cisco Remote Monitoring Suite (RMS).
- Also related is the documentation for Cisco CallManager.
- Technical Support documentation and tools can be accessed from
http://www.cisco.com/en/US/support/index.html
- The Product Alert tool can be accessed through
http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice

New and Changed Information

The following sections describe new features and changes that are pertinent to this release.

Overview

IP Contact Center (IPCC) Release 7.0(0) and Intelligent Contact Management (ICM) software Release 7.0(0) continue to build real value for both new and existing customers of Cisco's Customer Interaction Network solutions. Significant enhancements have been made across the solution suite:

- New, simplified deployment models for IPCC Enterprise, with a new web-based administration tool and streamlined installation (see System IPCC Enterprise Deployment, page 15)
- IPCC Gateway—extending the capabilities of ICM to 'child' IPCC Enterprise and IPCC Express installations
- IP Phone Agent—a high value package enabling customers to gain the benefits of IP Contact Center at a lower overall cost, allows an agent to log on and work from a Cisco IP Phone
- Improved Multi-tenancy for IPCC Hosted Edition
- Network Consultative Transfer (PSTN) for ICM Hosted and IPCC Hosted Editions
- Improved Customer Interaction Network Reporting
- Improved Upgrade process (see Upgrade, page 18)

On the base platform, we have added functionality that will enhance the overall fit into corporate networks:

- Support for Active Directory and Windows Server 2003
- Security hardening, encryption, Windows firewall support, and Quality of Service features
- Improved manageability with SNMP-based application health monitoring and extended functionality for ICM/IPCC Support Tools
- CTI OS support for Microsoft .NET

There are also several features that enable customers to integrate various Cisco IP Communications products seamlessly into their Customer Interaction Network:

- Cisco IP Communicator replaces Media Termination
- Support for Customer Voice Portal (CVP) 3.0 (for all IPCC/ICM Enterprise and Hosted Edition deployments, except for the System IPCC Enterprise deployment)
- Support for current versions of CallManager—see the *Cisco IP Contact Center Enterprise Edition Software Compatibility Guide* for a complete listing http://www.cisco.com/univercd/cc/td/doc/product/icm/ipccente/ipctt_cg.pdf

Considerable improvements have also been made on IPCC Enterprise and IPCC Hosted Editions, designed to increase the productivity of agents, supervisors, and contact center managers:

- Dynamic Agent Re-skilling
- Several new reporting templates, including graphic displays for trend analysis
- Outbound dialing enhancements
- Support for home based agents, either via broadband or ‘POTS’ phones
- Graphical real-time views of agent activity for supervisors

Overall, Release 7.0(0) is a significant step forward for both ICM and IPCC for superior productivity, ease of use, smooth migration from legacy platforms, and improved interoperability with other Cisco IP Communications solutions.

The following sections discuss the new features in Release 7.0(0) of Cisco's IPCC/ICM Enterprise and Hosted Editions software in more detail.

ICM Enterprise Edition

IPCC Gateway

IPCC Gateway extends ICM capabilities to Cisco’s IPCC. This new feature allows ICM to connect to multiple IPCC Enterprise or IPCC Express systems in a ‘child’ mode, enabling the ‘parent’ ICM to provide enterprise-wide routing and reporting—while still controlling its other ICM Peripherals, such as TDM ACDs. The ‘child’ IPCC system can automatically configure its agents and skills up to the ‘parent’ ICM.

Domain Security / Active Directory Support

ICM/IPCC can now operate in a shared corporate domain.

- Removes the requirement that the user running setup needs to have domain administrator privileges
- Provides a consistent set of permissions for all configuration, scripting and reporting tools
- Eliminates the use of generic names such as "SQLadmin", replacing these with product distinguished names
- Permissions can be assigned to organizational units within the domain instead of to the entire domain

Prior to Release 7.0(0), ICM and IPCC were required to be in their own Active Directory domain or forest.

The Release 7.0(0) support of Active Directory has wide-ranging implications, including pre-installation preparation, a requirement for native mode AD, and Organizational Unit (OU) allocation. The *Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* should be read with care.

In particular, it should be noted that there is **no** support for Windows NT Domain Controllers.

It is recommended that member servers use the AD Domain Controllers as their DNS servers.

Note that Release 7.0(0) requires the domain to be (at least) at Windows 2000 native mode—mixed node is NOT supported.

Add an Instance in ICM Setup; New Capabilities of ICMSetup in \icm\bin

Adding, editing, and deleting an ICM instance is now a standard part of ICM Setup.

In addition, many of the actions that could only be performed from the ICM Setup on the CD can now be performed from the Setup (called ICMSetup.exe) in the local \icm\bin directory.

For more information, refer to the *ICM Installation Guide for Cisco ICM Enterprise Edition*.

Security

Release 7.0(0) introduces a number of security features and improvements to protect the ICM/IPCC platform and data against mainstream attacks and other risks to a voice application such as ICM and IPCC. These features include:

- Automated Windows Server 2003 hardening provided by the Cisco ICM Security Template bundled with the ICM/IPCC and System IPCC software installers.
- Default configuration of Secure Sockets Layer (SSL) on WebView, Internet Script Editor, Agent Re-skilling, System IPCC Web Administration, and Support Tools Server Administration.
- Support for Windows Authentication (versus Mixed Mode) on SQL Server 2000 and 'sa' password protection.
- Support for Cisco Security Agent (CSA) version 4.5, leveraging its extended features in the standalone agent available for ICM and IPCC servers.
- Support for Windows Server 2003 SP1 and Windows XP SP2 Windows Firewall functionality. The Windows Firewall is automatically configured by the CiscoICMfwConfig utility on Windows Server 2003 SP1 and by the application installers on XP SP2.
- An expanded list of qualified Anti-Virus products now supported with the ICM and IPCC applications. The supported applications are McAfee VirusScan 8.0i, Trend Micro ServerProtect 5.58, and Symantec AntiVirus 9.0.
- Cisco ICM and IPCC applications also support the deployment of Host Based IPSec on Windows Server 2003 to secure data in transit such as call variables, Extended Call Context variables, configuration data and all communication along specified paths.
- Implementation of TLS in CAD and CTI OS (C++/COM Toolkit only) to secure communication from the agent desktop to the CTI OS Server to protect agent authentication credentials and all CTI data. The CTI OS TLS implementation supports mutual authentication and integration with a Public Key Infrastructure (PKI).
- Revamped *Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* as well as a complementary Security chapter in the *IPCC Solution Reference Network Design (SRND)* document.

Quality of Service (QoS)

QoS allows customers to more easily prioritize traffic on their network.

QoS is now supported on the dedicated ('private') network between duplexed pairs of Routers and of PGs (respectively):

- Replacing UDP heartbeats with TCP keep-alive messages
- Supporting layer 2 prioritization with 802.1p, a LAN QoS handling mechanism
- Supporting layer 3 classification with DSCP

See Quality of Service (QoS), page 30, for additional details.

Logger Efficiency Improvements

The Logger now handles configuration and historical data separately, so that configuration changes are no longer slowed down by historical data transfers. Similarly, in the case that historical data transfer temporarily fails, propagation of configuration changes will remain unaffected. Note that this combined functionality is still part of a single Logger node; that is, the externally visible functionality of the Logger remains essentially unchanged.

Dynamic Routing Client

When ICM uses the "translation route to VRU" method to route a call to a type2 SCI VRU, the VRU becomes the new routing client for the call. For Release 7.0(0) a new mechanism has been added in ICM to support a subsequent network transfer using that new VRU routing client. In an environment in which the original routing client is not capable of network transfer, all the pre-route calls can be transferred to CVP via Translation Route To VRU to take advantage of the network transfer feature.

This feature can be used in several scenarios:

- To support Transfer to VRU with Outbound for Hosted IPCC where a shared Network VRU is used for providing announcements to targeted phones/answer machines.
- To receive a call on an converged enterprise network after a carrier pre-route using CVP to control the call.
- To use pre-routing for load balancing purposes before the call is sent to a CVP controlled network, with call context and cradle to grave reporting capabilities.

Windows Operating System Support

For new installations, Release 7.0(0) ICM/IPCC Setup requires the installation of Windows Server 2003 SP1 (or later).

For Release 7.0(0) common ground upgrades (which are subject to a later update of the operating system), the SP4 requirement for Windows 2000 **must** be met. All components of Release 7.0(0), including CTI OS, have this common ground upgrade requirement.

Note that Windows 2000 Server is subject to end-of-life/end-of-support considerations as enforced by Microsoft.

Specific requirements, for new installations, technology refresh upgrades, and common ground upgrades, are found in the *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)* and the *ICM Upgrade Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

SQL Server Support

For both new installations and upgrades, Release 7.0(0) requires that SQL Server 2000 SP4 be used. ICM/IPCC Setup checks that you are using the appropriate version of SQL Server during Logger and AW (HDS) component setup.

Specific requirements, for new installations, technology refresh upgrades, and common ground upgrades, are found in the *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)* and the *ICM Upgrade Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

The 'Dynamic' memory setting is recommended for Logger and HDS.

ICM Hosted Edition

In addition to supporting the above listed (ICM Enterprise) features, ICM Hosted Edition also has the following enhancement.

Network Consultative Transfer

NCT allows geographically diverse call center agents to use the Service Provider's network to consult and transfer calls. Often referred to as a "warm" transfer, it removes the need for ACD tie lines to transfer calls. It supports an agent transfer to another agent without outpulsing additional digits. Note that this feature requires a specific ICM NIC software component.

IPCC Enterprise Edition

In addition to supporting the above listed ICM Enterprise features, IPCC Enterprise Edition also has the following enhancements.

- System IPCC Enterprise Deployment, page 15
- Connectivity to ICM Enterprise, page 16
- Split Cluster Support, page 16
- Dynamic Agent Re-Skilling, page 16
- Reporting Changes, page 17
- Outbound Support for Agent Re-Skilling, Sequential Dialing, Specific Buttons on CAD, page 17
- Increased Agent Extensions to 15 Digits, page 17
- Home Agent Support, page 17

System IPCC Enterprise Deployment

Release 7.0(0) introduces a new IPCC Enterprise variation targeted at simplified installations. Known as "System IPCC Enterprise deployment", the new pre-defined deployment models for IPCC Enterprise simplify system design and deployment planning and include a radically improved, web-based configuration feature.

The new software installation process for System IPCC Enterprise deployment models reduces typical software installation time for IPCC Enterprise to generally less than an hour.

The new IPCC Enterprise Secure Web Administration, available exclusively with System IPCC deployment models:

- Reduces complexity for IPCC Enterprise software configuration and administration
- Provides remote administration capability through a browser, and therefore does not require installing additional administration workstations

For more information, refer to the *System IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition*.

Connectivity to ICM Enterprise

IPCC Enterprise can now be connected to an ICM Enterprise system as an IP ACD to enable interoperability between IPCC Enterprise and other ACD systems. Additionally, this configuration can be used to connect multiple IPCC Enterprise systems. This capability is based on a new ICM Enterprise component, the IPCC Gateway, and a new IPCC Enterprise component, the System PG.

This feature provides:

- Improved migration capabilities for large enterprise customers with multiple ACDs
- Improved scalability for IPCC Enterprise deployments through the use of multiple systems
- Support for intelligent business segmentation, allowing the implementation of multiple distinct IPCC Enterprise deployments with distinct administration, routing and reporting; but also providing enterprise view reporting and call sharing with ICM
- Auto-configuration support reduces the need to perform dual administration between ICM and IPCC

Split Cluster Support

IPCC Enterprise can now be configured to support a geographically split CallManager cluster using a single logical peripheral (the CallManager appears as one system). This feature enhances IPCC Enterprise's industry leading fault tolerance architecture by providing a fully redundant ACD system with the software split between two regional/national data centers. Also called "clustering over the WAN".

Dynamic Agent Re-Skilling

For IPCC Enterprise, there is a new secure web-based interface for team supervisors that allows them to change agent skills and impact call routing in real time, that is, without requiring agents to log out and log back in to update skill group membership. (Note that supervisors can only perform changes on those agents that they supervise.)

This dynamic re-skilling is available no matter how you re-skill the agent; you can use the Agent or Skill Group Explorer in Configuration Manager, or the web-based interface. However:

- The web-based interface allows access from any machine with a supported browser (you need not install an AW on the machine to do agent re-skilling)
- The web-based interface provides a very focused view for supervisors, reducing the complexity involved in performing this specific task

Reporting Changes

See Reporting, page 19.

Outbound Support for Agent Re-Skilling, Sequential Dialing, Specific Buttons on CAD

- Dynamic Re-skilling of agents is supported in Outbound Mode. Blended Contact Centers can use this to move agents between Campaigns.
- The “Find Me” feature for Outbound Dialer allows the Predictive Dialer to find a customer by dialing up to 10 numbers for a single customer.
- Cisco Agent Desktop provides Outbound Specific buttons: Accept, Skip, Reject, Skip-Close, Reject-Close and Callback.

Increased Agent Extensions to 15 Digits

Agent extensions may be up to 15 digits (previously 9). This permits implementation of a global dial plan.

Home Agent Support

Support is provided for Remote Agents using IP Phones and/or PSTN phones over a Cisco Business Ready Teleworker setup. By means of this support, Cisco IPCC remote agents can benefit from standard Cisco 830 series router support, persistent VPN, Cisco IOS based security and QoS for voice over a VPN tunnel. A Home Agent using a PSTN phone does not require a Cisco 830 series router.

The following caveats and limitations exist for the IPCC Enterprise Remote Contact Center Agent

1. Network Address Translation (NAT) is supported when Remote Agent is used with the Cisco Business Ready Teleworker Model. (However, Silent Monitor—for both CTI OS and CAD—is not supported with NAT.) Design Guides for the Business Ready Teleworker can be found at:
   - http://www.cisco.com/go/teleworker
   - http://www.cisco.com/go/v3pn
   - http://www.cisco.com/go/srnd
2. Wireless access points are supported. Their use, however, should be determined by the enterprise security polices of the customer. Wireless use does not affect home agent performance since the bandwidth that wireless supports is greater than the broadband link. 7920 Wireless IP Phones are not supported.
3. Only one IPCC Enterprise Remote Agent per household is supported.
4. This Solution has only been tested with centralized IPCC Enterprise and Call Manager Clusters.
5. Routing through a Cisco 830 series with Firewall enabled is supported.
6. The G.729 codec is not supported for software conference bridges. Voice quality may degrade when the remote agent IP phone is configured using a G.729 codec and the agent enters a call manager software conference bridge. It is recommended that the conference bridge be configured on a DSP hardware device. There is no loss of conference voice quality using a DSP conference bridge. This is the recommended solution even for pure IP telephony deployments
7. The IPCC Enterprise server recognizes failures when the remote agent desktop or connection breaks. It will stop routing calls to that agent until the agent logs back in and goes to a ready call state. Callers will be routed to other available agents.

8. IP Communicator for CTI OS or CAD Desktops is NOT SUPPORTED for Remote Agents.
9. The only traffic that is marked for priority AF31 from the agent desktop is voice. CTI traffic and Desktop Application traffic is not marked. Voice gets the priority. CRM Desktops like Siebel and Oracle are supported, however Silent Monitoring and Recording is not supported for CRM Desktops such as Siebel, Oracle, and so forth. Silent Monitoring, both Desktop based and SPAN Port based, is not supported with CRM Desktops and will not work.
10. Media Termination for CTI OS and CAD is not supported.
11. CTI OS Agent Login may take up to 30 seconds. CAD Agent Login may take up to **2 Minutes**. Other operations such as Ready/Not ready are not impacted.
12. There may be times when the ADSL/Cable link goes down. When the link is back up, the Home Agent may have to reset their ADSL/Cable modem, 830 series router, and IP phone. The home agent must become familiar with restarting the 830 series router. Total time for the router to cycle is about 2 minutes. After which the home agent will have to re-login again for CTI application.
13. No special reports exist for individual remote agents. IPCC Enterprise Reports as it pertains to a Headquarter Contact Center are applicable.
14. Cisco CAD based IP Phone only agent and Cisco IP Phone control for CTIOS is NOT supported for remote agents.
15. Do not use soft VPN clients to establish VPN connectivity for remote agents with IP Phones. VPN connection has to be setup using hardware based VPN through a 830 series router.

IPCC Hosted Edition

IPCC Hosted Edition supports many of the above listed (IPCC Enterprise and ICM Hosted) features—such as Split Cluster Support, Dynamic Agent Re-skilling (though see Dynamic Agent Re-Skilling Restrictions for IPCC Hosted Edition, page 80), and Increased Agent Extensions—as well as supporting Outbound and Multi-channel Options in specific deployment models. IPCC Hosted Edition also has the following enhancement.

Improved Multi-Tenancy

Multi-tenant CTI OS is available for IPCC Hosted Edition. This enables efficient scalability for IPCC Hosted Edition installations when deploying smaller sized customer installations.

Upgrade

Significant changes have been made to the upgrade process for version 7.0(0). Logger and HDS data migration is now accomplished using a new tool, called the Enhanced Data Migration Tool (EDMT), which replaces the background data migration which occurred when upgrading to previous releases. The 7.0(0) *ICM Upgrade Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* has been rewritten to include more detailed upgrade procedures, and includes upgrade checklists to make it easier to keep track of progress during a system upgrade. The 7.0(0) *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)* also has been enhanced to include hardware definitions for both Technology Refresh (hardware replacement) and Common Ground (hardware reuse) upgrades.

For specifics on the upgrade process, refer to the *ICM Upgrade Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

For specifics on the hardware (including RAID) requirements, and on **Windows operating system requirements**, refer to the *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)*.

Reporting

WebView Deployment and Installation

WebView is no longer installed as an option on a Distributor AW, but is its own entity that can be installed on a separate server, and pointed at the Distributor AW. The WebView database remains on a Distributor AW with the configuration (awdb) and historical databases (hds). The *WebView Installation and Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* and the *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)* have been updated to describe how to deploy WebView given this new option, both procedurally, as well as from a planning perspective. WebView continues to communicate with all databases via ODBC. The former dblib-based backup connection functionality has been removed.

WebView can still be installed co-resident with a Distributor AW and is fully supported in that deployment. However, by separating WebView from the Distributor, one can deploy more WebView servers without adding more databases—and therefore support more total WebView users in the enterprise.

Stability and Serviceability Improvements

An additional service is now installed with WebView called the "Cisco ICM Jaguar WatchDog" and it will appear in the Services control panel. This process monitors the health of the Jaguar service, and by default will restart Jaguar if it detects a problem or finds the service has been stopped.

Logging and messaging have been improved in a number of areas within WebView. If a report query results in a SQL error, the actual error text is now returned to the user rather than a blank report. This error lets users know there was a problem and gives them information that can be passed along to technical support.

WebView now performs checking on the WebView database to ensure that it is the same version that it expects, and new messages have been added to indicate if there was a problem upgrading WebView, or if the WebView database is not reachable. If there is a problem with the WebView database, the features that depend on it are automatically disabled (saved reports, favorites, and scheduled jobs) and messages are provided to end-users.

Ease of Use Improvements

- WebView introduced a caching mechanism in prior releases that would allow both the pick-list of items and the template list to return more quickly to end users. By default, the cache would refresh itself every two hours. In this release, end-users are given the ability to refresh the cache on demand from within WebView. If a new element is configured (agent, skill, and so forth) or a new custom template is added, it can be seen instantly in WebView by refreshing the cache.
- For saved reports, when launched, the name of the saved report will appear in the title bar of the report window, followed by the template name. For ad-hoc reports only the template name will appear. This makes things easier to find when multiple windows are minimized.
- The Event Viewer has been enhanced to color-code errors and warnings, and provide summaries of each at the top of the page.
- The Job Scheduler now allows users to schedule any of their private reports, as well as any of their favorite reports.
- The "Schedule" category has been removed in WebView as it did not contain any standard templates. For customers who need to add this category back in order to support custom templates, the procedure for doing so is described in a Private Labeling whitepaper that is available upon request.

IPCC Gateway PG Reporting

The portfolio of ACDs across which ICM provides Enterprise Wide Reporting capabilities is now extended to include IPCC Express and IPCC Enterprise, when connected to ICM through IPCC Gateway.

Network Consultative Transfers

Agent and Skill Group reports which provide call count information on consultative, transfer, and conference calls now include network consultative transfer calls.

InfoMaker and WebView Infrastructure Upgrade

The reporting engine infrastructure (EAServer/PowerBuilder) is now upgraded to support the most recent version of Sybase InfoMaker for custom reporting purposes. For specific version information, see the *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)*.

InfoMaker is no longer supported for installation on the AW or WebView servers. It can be installed on a desktop computer for remote access to WebView. For details see the *Template Design Guide Using InfoMaker for Cisco ICM/IPCC Enterprise & Hosted Editions*. Customers who are upgrading from a previous release should verify all of their custom templates to make sure they behave properly with the new version of InfoMaker. It is important to test the templates in WebView, and ensure that header locking works correctly, that the reports appear as expected, that alignment is correct, and so forth.

WebView Changes for Partitioned Systems

Real time reports for enterprise level items (services and skill groups) display all the data related to those items, provided the user has permission to view the enterprise level items. In prior releases, the enterprise data included only the subsets for which the user had explicit permission. This is consistent with the way historical reports work in all releases.

For example: Consider a case where an Enterprise Service (esvc1) contains services svc1, svc2 and svc3. The WebView user (Domain1\User1) has been granted access to esvc1 and to svc1. This user runs an enterprise service real-time report selecting esvc1. In 5.0 and 6.0(0), the user would see records related only to svc1, while in 7.0(0), the user is able to see records related to all constituent services (scv1, svc2 and svc3).

Reporting Data Enhancements

In order to better meet reporting needs that are required to effectively run a call center, we enriched our database schema with new data fields. Some of this enhanced information is available on standard WebView templates, while other data enhancements can be used to build custom reports to meet your specific business needs.

The following are data enhancements that have been made in Release 7.0(0).

- Call Type Abandons
  Previous releases included (Router Task Aban & Delay Q Aband Time) all calls that abandoned at the CallType (that is, at the desktop while ringing, at the VRU (prompting) and abandons in queue). In Release 7.0(0), Call Type Abandon Data Enhancements have been made to provide visibility on calls (and associated duration) abandoned at VRU, calls that abandoned while ringing at the agent desktop, and calls that abandoned in Queue. Individual database fields have been added for each of these.
- Call Type Errors
  Prior to Release 7.0(0), only total error counts were provided independent of where the error occurred. Enhancements have been made in Release 7.0(0) to provide additional visibility into where the error occurred, to help narrow down and take corrective actions. The errors are now classified as follows:
  - Routing Errors: Errors that occur because of routing issues, for example, when a routing script fails to find a target.
  - Agent Errors: Calls that encountered errors at the agent desktop.
- Call Type VRU Tasks and Time
  Additional database fields have been added to provide real-time information on the total number of tasks and the total time at the VRU (for both prompting and queuing). Prior to Release 7.0(0), only the number of tasks in queue and queuing time at the VRU were available. These enhancements provide additional visibility toward identifying the number of tasks and how time was spent at a VRU (prompting or queuing).
- Call Type Tasks With IPCC Agents
  Enhancements have been to provide real-time information on the number of tasks that are with IPCC agents. This allows real-time monitoring to identify the number of tasks agents are currently working on.
- Skill Group Service Level Statistics
  In order to provide additional visibility into relative performance of skill groups in their ability to meet service level targets, Skill Group Service Level statistics have been added to the schema (ServiceLevelCalls, ServiceLevelAbanCalls) similar to Call Type Service level statistics. IPCC customers have the ability to setup SL thresholds for individual Skill Groups and collect the service

level data. The WebView Skill group templates have been enhanced to provide the number of calls that were answered and abandoned within the Service Level threshold. Custom reports can be developed to reflect Service Level calculations that meet your business needs.

Also see ICM Database Schema Changes, Release 6.0(0) to Release 7.0(0), page 41.

Terminology Clarifications in Templates

The following enhancements have been to provide terminology clarifications for Release 7.0(0).

- In Call Type, Service and Route templates, the column header "OverFlowOut" and "OverFlowIn" are changed to "Flow Out" and "Flow In" respectively. This was done to more accurately describe what these columns represent (that is, the number of calls that were redirected from one call type/service/route to another as part of call flow or script logic). As part of gathering reporting statistics in ICM/IPCC, we often provide scripting guidelines to change call types. For example it is recommended that you create separate call types for information gathering (Info_Call_Type) and queuing (Queue_Call_Type) statistics and changing the call type in ICM/IPCC scripts prior to queuing. In this example, the "Flow Out" column in call type template will reflect the number of calls that flowed out of "Info_Call_Type".
- In Agent templates, the column header "Aban While Offer" is now changed to "Aban Ring", to be consistent with other templates and also to more accurately describe what the column represents (that is, the number of calls that abandoned while ringing at the agent desktop).
- The column header "Direct In" in agtskg21 and agtskg22 has been changed to "Internal In" to be consistent with other templates.
- The column header "Hold" in agent reports (agent/agtskg/agteam/agtper – 21/22) is now changed to "All Hold" to more accurately indicate that this column represents all calls (Incoming/Handled, External and Internal calls) that were put on hold. In other agent reports the context for the held call is provided as part of the headers/super-headers appearing in the templates, for example, "Incoming Hold".

Enhanced Templates

The following templates are those that have been enhanced for Release 7.0(0).

Agent Templates

- **agtskg20: ICM Agent Skill Group Real Time** template was used for ICM and IPCC prior to Release 7.0(0). For Release 7.0(0), there are two templates—one for ICM (**agtskg20**) and one for IPCC (**agtskg30**). The template columns which are only applicable to IPCC are not shown in the ICM version.

Note If users have saved reports and favorites based on this template, and are running in an IPCC environment, those saved reports should be deleted and re-created with the new IPCC-specific template.

- New template column that provides the extension that the agent used at the time of Logout has been added to the following agent templates:
  - agent03: Agent Media Logout Status
  - agtper03: Agent Peripheral Media Logout Status

- agteam03: Agent Logout Status

Skill Group Templates

- **perskg04, perskg20-26, entskg04 and entskg20-26: Peripheral Skill Group and Enterprise Skill Group** templates were used for ICM and IPCC prior to Release 7.0(0). For Release 7.0(0), there are two sets of templates—one for ICM (**perskg04, perskg20-26, entskg04, entskg20-26**) and one for IPCC (**perskg14, perskg30-36, entskg14, entskg30-36**). The template columns which are only applicable to IPCC are not shown in the ICM versions.

Note If users have saved reports and favorites based on these templates, and are running in an IPCC environment, those saved reports should be deleted and re-created with the new IPCC-specific templates.

- New template columns have been added to the following templates that provide information on the number of calls that were answered and abandoned within the Service Level threshold for the skill group.
  - perskg30: IPCC Peripheral Skill Group Status Real Time
  - perskg35: IPCC Peripheral Skill Group Consolidated Half Hour
  - perskg36: IPCC Peripheral Skill Group Consolidated Daily
- **perskg25/25/35/36 and entskg25/26/35/56 Peripheral Skill Group and Enterprise Skill Group** templates have been modified to now include the "Average Speed of Answer" (ASA) column.

Call Type Templates

- **caltyp20: Call Type Real Time** template has been enhanced to provide additional information on the number of calls that are at the VRU (Prompt or Self Service), number of calls in queue and the number of calls that are with IPCC agents.

Enterprise Skill Group Templates

- Enhancements have been made to **entskg21-26** templates to provide aggregated information for enterprise skill groups instead of providing details for the individual peripheral skill groups that belong to the Enterprise Skill Group. In other words, the reports now provide one row for the selected enterprise skill groups.
- New template column "Incoming Held Tasks" have been added to **entskg06** and **entskg07** templates. In addition, enhancements have been made to change the calculation for "Avg.Hold Time" to provide the average hold time for incoming tasks that were put on hold instead of providing the average for all incoming tasks irrespective of the tasks being on hold or not. The column headers were also enhanced to reflect the changes.

For more information, refer to the WebView online help and to the *WebView Template Reference Guide for Cisco IPCC Enterprise & Hosted Editions*.

New Templates

The following templates are those that have been added for Release 7.0(0).

Template	Description
Agent Skill Group Assignments (agteam29)	Real-time Agent Team template that provides information to supervisors on the number of agents on their team and their current skill group assignments.
Agent Team State Count Real-Time (agteam32)	Real-time Agent Team template that shows a summary of total number of agents that belong to a team, assigned team supervisor, number that are logged on, number of agents in each of the different states, and number of agents that are eligible to receive a task.
Call Type Queue Status Real Time (caltyp25)	Real-Time Call Type Graphical templates that show queue length and number of calls in the queue that are inside/outside SL threshold.
Call Type Tasks Offered Over Half Hour (caltyp26)	Real-Time Call Type Bar Chart that provides information on the number of tasks offered to specified call types in the current half hour interval.
Call Type Queue Delay Status Real Time (caltyp27)	Allows monitoring of customer experience while waiting in queue, such as average time spent in queue, longest task in queue, and the average speed of answer.
Call Type Task Status Now Real Time (caltyp28)	Real-Time Call Type Bar Graph that allows monitoring of number of tasks at VRU (Prompt or Self-Service), number of tasks in Queue, and number of tasks currently with IPCC agents.
Call Type Service Level Abandons Daily (caltyp37)	Provides a graphical representation of trends in the number of abandoned calls within the call type service level threshold, for selected call types.
Agent Team Incoming/Outgoing Task Durations With Agent Detail Half Hour (agteam33) [**though documented in the 7.0(0) manuals, this template will only become available in a subsequent Service Release**]	Table of task durations for incoming and outgoing tasks handled by agents in a team by half hour. This template provides information on inbound and outbound task counts, average durations, and total durations for agents in selected teams.
Agent Team Incoming/Outgoing Task Durations With Agent Detail Daily (agteam34) [**though documented in the 7.0(0) manuals, this template will only become available in a subsequent Service Release**]	Table of task durations for incoming and outgoing tasks handled by agents in a team by day. This template provides information on inbound and outbound task counts, average durations, and total duration for agents in selected teams.
Agent Team Incoming/Outgoing Task Durations Half Hour (agteam35) [**though documented in the 7.0(0) manuals, this template will only become available in a subsequent Service Release**]	Table of task durations for incoming and outgoing tasks handled by agent teams by half hour. This template provides information on inbound and outbound task counts, average durations, and total duration aggregated for the individually selected teams.
Agent Team Incoming/Outgoing Task Durations Daily (agteam36) [**though documented in the 7.0(0) manuals, this template will only become available in a subsequent Service Release**]	Table of task durations for incoming and outgoing tasks handled by agent teams by day. This template provides information on inbound and outbound task counts, average durations, and total duration aggregated for the individually selected teams.

For more information, refer to the WebView online help and to the *WebView Template Reference Guide for Cisco IPCC Enterprise & Hosted Editions*.

TDM ACDs

Nortel Activity Code Support

Allows supervisors to track and report on agent activity when they go into a “not ready” state.

- Nortel Activity Code for agent state changes is now supported by ICM
- Agent state reporting templates can be used to report on these codes

Support Tools and Serviceability

Support Tools 2.0

Cisco Support Tools 2.0(0) is a suite of over fifty utilities that allows you to manage and troubleshoot the ICM nodes which process call load, routing, and reporting. Through Support Tools, you can troubleshoot configuration and performance problems on these systems from a single machine in your network, the Support Tools Server. Access to utilities in the Support Tools suite is through a browser-based interface—the Support Tools Dashboard—installed on the Support Tools Server. Levels of security control both access to the Dashboard and the ability to use specific tools once logged in. In low bandwidth conditions (for example, via dialup access) or when web browsing is otherwise impractical, most Support Tools utilities can also be accessed and run via command line.

The Support Tools suite includes the full set of standard diagnostic tools delivered with earlier ICM versions. It also provides key new functionality. This functionality includes:

- The ability to interrogate individual ICM nodes for their hardware/OS, Cisco component, and third party product information, and application specific data or files. New in this release is the ability to interrogate CRS (this includes IP IVR and IPCC Express), CVP, CAD, and IPCC Gateway.
- The ability to view, start, and stop services running on ICM nodes.
- The ability to view and terminate processes running on ICM nodes.
- The ability to compare and synchronize registry settings from different ICM nodes. New in this release is an improved display of only the registry differences.
- The ability to pull logs from most Cisco nodes including ICM CallRouters, Loggers, PGs, AWs, CTI OS, CCS, CEM, CMB, and CallManager. New in this release is the ability to pull logs from CRS, CAD, CSA and CVP.
- The ability to perform enhanced time-synchronized merged logging across servers.
- New in this release is the ability to raise trace levels when collecting logs and the ability to restore trace settings after log collection completes.
- The ability to run a majority of the tools in either Interactive Mode (where one system is immediately queried) or, new in this release, Batch Mode (where several systems can be scheduled to be queried at some point in the future).

Enhanced SNMP Support

ICM/IPCC 7.0(0) includes a number of enhancements to its Simple Network Management Protocol (SNMP) health monitoring and instrumentation features:

- A new agent supporting SNMP v1, v2c and v3 as well as several of the highly secure authentication and encryption protocols offered for SNMP v3.
- A new Contact Center Management Information Base (MIB) with instrumentation specific to ICM and IPCC. This new CISCO-CONTACT-CENTER-APPS-MIB provides explicit support for monitoring the health of the core components of ICM/IPCC.
- Support for IETF standard MIBs: HOST-RESOURCES-MIB and SYSAPPL-MIB.
- Integration with the CiscoWorks IP Telephony Environment Monitor (ITEM) network element management software.
- A new Microsoft Management Console (MMC) snap-in, the Cisco SNMP Agent Management snap-in, which can be used to configure the Cisco Contact Center SNMP Management component.

The SNMP components are now installed (though not configured) by default. Please refer to the *SNMP Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for more details.

Localized Features

The following product feature user interfaces are localized in IPCC/ICM 7.0(0) (with the exception of System IPCC Enterprise deployment, which initially offers only an English user interface):

Feature	Languages Available
Reporting UI and Templates	Japanese, European French, Canadian French, Simplified Chinese, Korean
Script Editor and ISE	Japanese, European French, Canadian French, Simplified Chinese

The following product feature Help is planned to be localized in a succeeding IPCC/ICM 7.0(0) Service Release:

Feature	Languages Available
Reporting Help	Japanese, European French, Canadian French
Script Editor Help and ISE	European French, Canadian French

Use of ICM language support requires that:

1. ICM is installed on a localized operating platform (for example, Japanese Windows Server 2003).
2. The correct language is selected in AW Setup.

Further information can be found in the *ICM Installation Guide for Cisco ICM Enterprise Edition*.

Technical Changes and Notes

The following items are generally of a more technical nature than those above.

IPCC 7.0(0) Support for CallManager 4.0(2) and 4.1(3) Features

IPCC 7.0(0) supports the following features in CallManager 4.0(2) and 4.1(3):

- Conference and Join
- Drop Any Add-Hoc Conference Party
- Media Termination at Route Point
- Multiple Calls Per DN
- New Conference Controller
- Security: Device Authentication
- Single Step Transfer
- Transfer and Direct Transfer
- Transfer to Voicemail

IPCC 7.0(0) DOES NOT support the following features in CallManager 4.0(2) and 4.1(3):

- Auto Update API
- Barge/Privacy Event Notification
- Call Distribution - Hunt List
- Call Park and Pickup

- QSIG: inter-operability with server TDM switch
- Security: Media Encryption
- Share line
- SIP signaling trunk

Cisco Discovery Protocol (CDP) Support Restricted to MCS Hardware

The Cisco Discovery Protocol driver, which supports discovery of Cisco Contact Center Servers, can be installed on MCS servers supported for the 7.0(0) release. The CDP driver periodically broadcasts CDP messages on active network interfaces. Any Cisco device with CDP support can locate a Cisco ICM/IPCC server by listening for these periodic messages.

The Cisco Discovery Protocol driver that had been provided on the ICM software CD (separate from ICM Setup) has been removed. In ICM 7.0(0), the updated CDP components, as well as an installation script, are placed on the server in the ICM\SNMP directory. Administrators may install CDP on Cisco MCS servers manually (except for System IPCC Enterprise deployment) using the CDPINSTALL.BAT script. Since the driver is only compatible with specific network interface chipsets, installation is highly discouraged on non-MCS servers as doing so may cause instability in the operating system.

Note Since System IPCC Enterprise deployment is supported only on MCS hardware, the CDP driver is installed on System IPCC Enterprise deployment servers as part of the normal software installation.

In addition to the CDP driver, the enhanced SNMP support also includes an SNMP subagent which supports the Cisco Discovery Protocol MIB (CISCO-CDP-MIB). The CDP SNMP subagent is installed by default by the ICM Setup program.

Cisco Security Agent (CSA) for Release 7.0(0)

A newer version of CSA, based on CSA engine version 4.5.1 and ICM CSA Policy version 2.0.0, is available for ICM/IPCC Enterprise Release 7.0(0). CSA 4.5.1 is compatible with both Windows 2000 Server SP4 and Windows Server 2003 SP1 running ICM/IPCC 7.0(0) applications. CSA 4.5.1 provides enhanced security as compared to its previous release, CSA 4.0. It no longer stores the CSA version information in the registry, instead the CSA version is available via the new agent GUI. The red flag system tray icon now indicates the state of the service. The responses to user queries can now be cached permanently, persisting across reboots. For more details refer to the *Cisco Security Agent Installation/Deployment Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.0(0)*.

CSA 4.0, which was supported on prior releases of ICM/IPCC Enterprise, is not supported on the 7.0(0) release. Hence, you must uninstall CSA 4.0 prior to upgrading ICM/IPCC Enterprise to the 7.0(0) release. For more details refer to the *ICM Upgrade Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

To use Cisco Security Agent, you must always use the default directories when installing any software on a server. You need not choose the default disk drive if an option is available (for example, C: or D:), but you must use default directories. Cisco Security Agent leverages rules which incorporate path information. Application actions may be blocked if the application is not installed in the correct directory. For this reason, it is mandatory that applications are installed in the default directories provided by the application installers. As just stated, drive letters are not restricted.

It is required that the CSA service be Stopped before you perform any install or upgrade activity. The CSA service can be stopped or started from the Windows Service Control Panel. Unlike CSA 4.0, there is no need in CSA 4.5.1 to suspend the CSA service before stopping it. In the 7.0(0) release, ICM Setup as well as System IPCC Setup automate the stopping and starting of the CSA service. Setup for other ICM Server Applications/Options (CTI OS, Support Tools, and so forth) warns the user to stop CSA, and a manual stop/disable of the CSA service is required. CSA does not protect the host while the service is stopped. The CSA service should be enabled/started after the install activity is over. It is strongly recommended that this practice also be followed during other installation and upgrade activities, such as for supported third-party products.

CSA support for the ICM Network Gateway (SS7 Gateway Node) is added with the 7.0(0) release (beginning with the CSA 4.5.1 engine).

ICM Setup Checks 'sa' Account Password

ICM 7.0 Setup checks for blank MS SQL Server 2000 "sa" account passwords. Leaving this password blank is a severe security hole that has already been exploited by the slammer worm. When a user installs Microsoft SQL Server 2000, that setup warns against leaving the password blank, but still allows a user to override the warning.

Most, perhaps all, customers will have already set the password before installing ICM. To be secure, ICM Setup checks the password value. If it is not blank, the password is not changed. If it is blank, then the sa password is set to a random string of 6 characters from the following sets ([a-z] [A-Z]). A dialog in Setup displays the following text: "The Microsoft SQL Server sa password was found to be blank. For your protection, the sa password has been set to this random string: xxxxxx. This password will not be displayed again, so please record the value if you use the sa login."

The sa account is not needed if all access to the system is through Windows Authentication. If a database administrator wants to use the sa account, and does not know the random password, the administrator can still change it by logging into the SQL Server using Windows authentication.

Note that Cisco recommends that users configure SQL Server to use “Windows Only authentication” versus “mixed mode authentication”. Please refer to the *Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for more information.

Quality of Service (QoS)

ICM Release 7.0(0) supports DSCP (Diffserv Codepoint) marking, and if deployed with Windows Packet Scheduler, 802.1p marking and traffic shaping for both the private and public network interface.

Enabling ICM QoS with Windows Packet Scheduler requires that the NIC adaptors NOT be configured with more than one IP address because of a restriction in the Windows Packet Scheduler. Refer to Microsoft knowledge base article 892494.

Another restriction of using Windows Packet Scheduler is that the shaping bandwidth reservation cannot exceed 80% of the NIC bandwidth, and this may limit the number of customer instances to be installed in a hosted environment.

Note that the use of UDP heartbeat is replaced with TCP keep-alive when QoS is enabled in ICM.

Secure Socket Layer (SSL) Changes

The ICM and IPCC web-based applications are all installed enabled with SSL with a self-signed server certificate by default on Windows Server 2003 (except for multi-channel applications). SSL is only enabled by default on WebView for the authentication of user credentials. WebView users will need to change the web server address (URL) of the WebView server to start with "https://" instead of "http://". Bookmarks may also need to change after upgrading to Release 7.0(0).

The default SSL settings are configurable using the SSL Encryption Utility (\icm\bin\sslutil.exe) which is installed on a Distributor or Administrative and Reporting server. For example, this multi-instance aware application can be used to enable SSL for the full reporting session on WebView. It can also be used to administer the self-signed certificate installed by Setup.

Windows Server 2003 SP1 Firewall Behavior

Windows Server 2003 SP1 introduced a new host-based firewall functionality which is supported by the ICM suite of applications. Windows Firewall is a protective boundary that monitors and restricts traffic that travels between a server and a network. It provides a line of defense against unauthorized users, malicious applications or unsolicited traffic. When properly configured, it can allow application or port based exceptions. The ICM product ships with a configuration utility that can be used to configure the Windows Firewall on the application server it is installed on. The list of supported applications can be found in the Windows Firewall Configuration chapter of *Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*. Please note that no other host-based firewall is supported, especially running alongside Windows Firewall. Host firewall implementations vary widely and there is no guarantee that a non-Microsoft host firewall and Windows Firewall will work well together. Cisco has only qualified the Windows Firewall.

There are a number of areas which must be carefully reviewed before enabling the Windows Firewall using the Configuration Utility provided (CiscoICMfwConfig).

- Make sure the Windows Firewall/Internet Connection Sharing service (sharedaccess) is running before any programs or system services listed in the program exceptions list are started. If you start the Windows Firewall/Internet Connection Sharing service after you have started programs that are listed in the Windows Firewall exceptions list, restart your computer and then start your programs and system services. Windows Firewall cannot track the state of a program's traffic if the program is started before you start the Windows Firewall/Internet Connection Sharing service. This will lead to the dropping of traffic targeted to a specific application or port, even though this application/port exists in the exception list.
- If the Windows Firewall service cannot start, all incoming connections are refused until the Windows Firewall service starts successfully. Check whether the Windows Firewall is either disabled or started to help determine the possible cause of a network communications failure. The Windows Firewall log file can be a good reference to determine what if any traffic is getting dropped. More on this can be found in the *Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.
- The Windows Firewall may mask network problems due to configuration errors, for example: A computer was attempting to send traffic from its private interface (2nd NIC) to its public interface's network but was unable to do so because of a mis-configured system that had not been setup with static routes.

Windows Firewall and Cisco Security Agent (CSA) Compatibility

Standalone Cisco Security Agent (CSA) version 4.5.1.616 policy 2.0.0 for Cisco ICM/IPCC Enterprise and Hosted Editions 7.0(0), when run concurrently with the default Windows Firewall, will disable the Windows Firewall. Since CSA utilizes firewall-like components, it will disable the currently running Windows firewall. This occurs each time the system is rebooted, even if the Windows Firewall has been enabled since the last system startup on Windows Server 2003 SP1 using the Cisco ICM Firewall Configuration Utility (CiscoICMfwConfig).

CSA provides host based protection for various resources on the system, such as files, registry, and network stack. CSA can also be tuned to control network access and act like a firewall. However, the standalone CSA 4.5.1.616 policy 2.0.0 for Cisco ICM/IPCC Enterprise and Hosted Editions 7.0(0) does not exploit this feature. Instead, Cisco ICM software supports the configuration of the Windows Firewall on Windows Server 2003 SP1 using a Windows Firewall Configuration Utility called CiscoICMfwConfig. Microsoft has recommended (as noted in the help guide for the Windows Firewall) that two firewalls should not be running at the same time due to potential configuration compatibility issues. However, since standalone CSA for Cisco ICM/IPCC Enterprise and Hosted Editions 7.0(0) software does not implement the firewall functionality of CSA, the Agent can coexist with the Windows Firewall in Windows Server 2003 SP1. An enhancement request (CSCsb48526) has been created against the Cisco Security Agent to not disable the Windows Firewall when CSA's firewall feature is not employed. In the interim, a workaround is provided. This workaround can be found in **Field Notice: Cisco ICM Enterprise & Hosted Contact Center Products Notice for Cisco Security Agent 4.1.5.616 policy 2.0.0** (http://www.cisco.com/warp/public/770/fn62188.shtml).

Note Both CSA and Windows Firewall protection for Cisco ICM software is recommended, but not required, by Cisco. If you do not use either CSA or Windows Firewall, or use only one of these, the issue discussed above does not arise.

Security Hardening Automation and Best Practices

In a Windows Server 2003 environment, ICM Setup and System IPCC Setup prompt the user to apply Windows Server hardening by default. Applying hardening ensures that the operating system is secure and protected against a number of vulnerabilities. The hardening provided is specifically customized to be compatible with the applications that may be installed on the server. The list of applications supported to run co-resident with a hardened ICM/IPCC system are: CTI OS, CAD, CSA, Support Tools, Media Blender, and of course all ICM and System IPCC Enterprise deployment software components. Refer to the *Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for more information.

A Prompt for Security Hardening checkbox is provided as part of ICM Setup. If the box is checked—and if security hardening has not been applied, or if an updated template is available—each time that Setup is run, you are prompted to apply security hardening.

Both of the just-mentioned features are available only on Windows Server 2003 systems.

The *Security Best Practices for Cisco Intelligent Contact Management Software Release 6.0(0) & 5.0* manuals remain relevant for the Windows 2000 common ground upgrade customer.

GEODES.DLL

Due to the newly acquired export classification for the Cisco ICM 7.0(0) product family to include high-encryption algorithms, the GEODES.DLL installed on a CallRouter with the MCI NIC or the CallRouter with the Application Gateway option is now the high encryption library. Upon upgrade for those systems relying on this library, no further steps are necessary to replace the older default file with the high-encryption one.

McAfee Anti-Virus Software Compatibility

Due to a defect encountered with the McAfee Anti-Virus product, VirusScan versions 7.x and 8.0i, systems with this product must be updated with the latest virus definition files before installing ICM software. Failure to do so will lead to one of the files that get installed by ICM/IPCC software Setup to be detected as a virus. This is a false positive and can be avoided by simply following staging best practices and updating the AV product, preferably both the scan engine and the virus definition files (DAT), as part of server staging.

Obsolete NICs Removed

The following ICM network interfaces (NIC software components) are no longer supported as of Release 7.0(0): BT INAP, BTV2 INAP, Concert, Deutsche Telekom, Energis INAP, France Telecom, ICRP, Telfort INAP.

- NAM-installed NICs that are being obsoleted all have an identified replacement (SS7IN) **or** are being obsoleted due to End-of-Life. See the *Pre-installation Planning Guide for Cisco ICM Enterprise and Hosted Editions* for specific information.
- The configured "client type" on the CICM INCRP NIC will show the residual numeric value of the prior (not removed) NAM NIC when NAM upgrade transitions.
- The CICM INCRP NIC "client type" should be reconfigured as part of the upgrade to align with the NAM NIC that is replacing the obsoleted NIC.
- NAM / CICM upgrades can occur in either order but no more than one major or minor version back.

Router Service Indication

When one of a duplexed pair of CallRouters is brought back into service, it must synchronize with its running partner. This may cause a brief disruption of service on the running Router, as it snapshots its state for transmission to the new Router. In order to minimize the disruption, the Router informs the NIC of the temporary situation, with an estimate of how long it will last. The NIC uses this information to maintain its connection with the network, even though the Router is unavailable. When the Router has completed the snapshot, it informs the NIC that it is available, and normal processing begins.

If the Router does not complete the snapshot within the configured time limit, the NIC disconnects from the network.

If this feature is not enabled, the NIC drops its connection to the network immediately, as in prior releases.

The default time is 15 seconds.

The relevant registry keys are:

Router\CurrentVersion\Configuration\StateTransfer\NICDefaultRoutingEnabled
(bool) default true

Router\CurrentVersion\Configuration\StateTransfer\NICDefaultRoutingSeconds
(int) default 15

This feature is available on selected NIC interfaces.

Multiple NAM: Provisioning NAM Replication Problem

After installation of a slave NAM, the NICR Replication process fails and restarts. The error in the log is "DB-Lib User Error: Login incorrect."

The workaround is to use the following manual procedure for granting replication rights on a provisioning NAM to a slave NAM:

1. Open an Active Directory Management Console (AD MMC).
   - A domain contoller will have a defined AD MMC under "Start|Programs|Administrative Tools".
   - Member servers may have had an AD MMC shortcut saved in "Start|Programs|Administrative Tools". To create a new AD MMC:
     Choose "Start|Run" and enter MMC to bring up a new console.
     On the main menu choose "Console|Add/Remove Snap-in...".
     Click on "Add", then choose "Active Directory Users and Computers".
     Click "Add" then "Close" to close the popup dialog.
     Click "OK" to close the "Add/Remove Snap-in" dialog.
2. To save this console for future use, go to the menu item "Console|Save as".
   - Connect to the target domain.
   - In the left pane, under the "Console Root" folder, right click on "Active Directory Users and Computers".
   - Select "Connect to domain".
   - Browse to the domain containing your ICM instances.
   - Expand the tree nodes to find the "Cisco_ICM" OU (the icon looks like a folder containing a folder).
3. Find the name of the slave NAM service Security group you want to grant access to.
   - Expand the "Cisco_ICM" OU node, then expand the facility OU node containing the instance OUs.
   - Select the slave NAM instance OU node.
   - Identify the slave NAM's service security group:
     The name of the group will end with "_Service".
     The description of the group will be "ICM Service Accounts".
4. Add the slave NAM Service Security Group to the provisioning NAM Service Security Group.
   - Select the provisioning NAM instance OU node.
   - Identify the provisioning NAM's service security group:
     The name of the group will end with "_Service".
     The description of the group will be "ICM Service Accounts".
   - Right click on the provisioning NAM's service security group. Select "Properties".
   - Click on the "Members" tab.
   - Click on the "Add" button.
   - Find and select the previously identified slave NAM service security group.

- Click on "Add", then click on "OK".
- Click on "OK" to close the properties dialog.
- Configuration is complete. Close the AD MMC application (saving MMC configuration on exit is optional).

MCS-7845I / MCS-7845-I1-CC1 NIC Controller PnP Issue

The way that Windows enumerates the dual NICs on the MCS-7845-I1-CC1 with a particular revision of the Broadcom chipset is incorrect. A command line patch can be run to fix this issue so that when events show up through the hardware monitoring software, you have the right NIC identified. Running the utility works fine whether the issue is present or not. The utility only changes settings if it detects things are wrong.

The problem is somewhat different on Windows Server 2003 (versus Windows 2000), but the remedial patch is equally effective. When additional NICs that have standard Windows drivers are installed prior to installing Windows, they will appear first, before the Broadcom NICs. Once the patch is run, you may now have two connections labelled Local Area Connection, and two named Local Area Connection #2. Functionality will not be impaired, but the system will be confusing. At this point, the additional NICs should be manually renamed using Network Connections in Windows and right clicking Rename to name these Local Area Connection #3 and #4. They can be identified by right clicking the individual connections and selecting properties.

After running the patch, you will need to reboot. The patch does not send back any messages after it is run, but the system needs to be rebooted following it.

The patch can be accessed from
www.cisco.com/pcgi-bin/tablebuild.pl/unity-util

Download and read the file Readme_NicNameX-Utility_PCD.txt.

Download nicnamex.zip and unzip it. Then, in accordance with the instructions in the Readme file, run NicNameX.exe.

Removal of Support for Ataman Telnet Daemon

The Ataman Telnet Daemon is not supported, and has been removed, in Release 7.0(0).

New Global Performance Monitor Collection Feature

With Release 7.0(0), the Node Manager process captures performance related data from the machine. This includes any machine on which one or more ICM node(s) are installed. This feature is turned on by default. The logs are captured in a CSV format in ICMROOT\log folder. Counters are captured at every one minute interval. Configuration settings for file size and number of files to keep in the log directory can be changed through the registry. By default the following counters are captured:

\Memory\Page Faults/sec
\Memory\Committed Bytes
\Memory\Pages/sec
\Process(_Total)\Handle Count
\Processor(_Total)\% Processor Time
\System\Threads
\System\Processor Queue Length
\System\Processes

MDS Performance Monitoring

Three Windows Performance Monitoring tools (PerfMon) objects are added for MDS performance monitoring. They are:

- MDSPROC—which contains counters of queuing to the duplexed side
- MDSPROCCLIENT—which contains counters of queuing from the MDS to a specified MDS client
- MDSCLIENT—which contains counters of queuing from an MDS client to the MDS.

To enable MDSPROC and MDSPROCCLIENT, add the registry value EnablePerformanceMonitor under MDS\CurrentVersion\Process and set it to 1.

To enable MDSCLIENT for a client, add the registry value EnablePerformanceMonitor under MDS\CurrentVersion\Clients\[client-id] and set it to 1.

The registry change is dynamically effective.

MBUF Buffer Memory Management

The MBUF Buffer Memory Management is improved with the following changes:

- An adaptive algorithm is implemented for managing buffer limit. The overall buffer limit is set as a percentage of system RAM, and an ICM/IPCC process dynamically expands or shrinks its quota.
- The free-lists (also known as application-layer buffer caches) are removed, and buffers are allocated from system heap directly.
- The old registry values BufferLimit, BufferMaxFree and BufferMaxQueuePercent are removed. The new registry settings are centralized on per system basis under ICM\SystemSettings\MBufMemLimit.

PG Process EMS Display Output Suppressed

For the ICM service windows that run on the system servers, tracing will not be displayed for the following processes in the interest of performance. Tracing is controlled via registry key, and can be enabled for select trouble shooting circumstances if required. The relevant registry key name is EMSDisplayToScreen.

Here is the list of processes where Display to Screen will be disabled on new installations:

Acmipim (PIM process used for IPCC Gateway)
Badialer (Dialer process Used for Outbound Option)
Eapim (PIM process used for IPCC Enterprise and System IPCC Enterprise deployment)
Jtapigw (JGW process used for IPCC Enterprise and System IPCC Enterprise deployment)
CTI Server (Common CTI Interface Process used for all PGs)
Campaign Manager (Process Used for Outbound Option hosted on the Side A Logger)
Campaign Import Process (Process Used for Outbound Option hosted on the AW/HDS)

Dynamic Agent Re-Skilling URL Is Missing when Installed with ICM Setup

In an IPCC Enterprise system installed with ICM Setup, the documented link to the Dynamic Agent Re-skilling web page does not work. The URL "https://<host>/reskill" returns "The page cannot be found".

Use the following URL instead:

https://<host>/uiroot

where <host> is the name of the Admin Workstation on which Dynamic Agent Re-skilling was installed.

Web-Based Dynamic Agent Re-skilling Can Get Disabled on Rerunning ICM Setup

After running ICM Setup in edit mode to modify an AW Distributor component with Dynamic Agent Re-skilling enabled, Tomcat services are unable to start, causing web-based Dynamic Agent Re-skilling not to work. In the icmsetup.log file, the following error appears:
"Could not rename C:\icm\tomcat\conf\server.xml.custom to C:\icm\tomcat\conf\server.xml".

This problem occurs after editing an already installed AW Distributor component with Dynamic Agent Re-skilling enabled. This problem occurs for IPCC Enterprise/Hosted Editions, though not for System IPCC.

- If you plan to use ICM Setup to modify an AW distributor with Dynamic Agent Re-skilling enabled, first save a copy of C:\icm\tomcat\conf\server.xml to another location, and copy it back when setup is complete. Then start Apache Tomcat from the Windows Services control panel.
- If you do not discover this problem until the problem has already occurred, and if there are no engineering specials (ESs) or service releases (SRs) applied to the system, you can correct the problem by running Setup from the ICM Software CD, and re-editing the AW component—in particular, checking the **Agent Re-skilling Web Tool** feature again. (If you do have an SR or ES installed, you must uninstall it before running Setup. After running Setup, reinstall the SR or ES.)
- Alternatively, if you do not discover this problem until the problem has already occurred, you can copy server.xml from another valid installation of a 7.0(0) AW distributor with Dynamic Agent Re-skilling enabled to C:\icm\tomcat\conf\server.xml, if you have such an installation available.

System IPCC and Database Installation

It was not initially documented in the *Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* that System IPCC servers must **not** be partitioned.

If you have partitioned your System IPCC server, the System IPCC installer may report the following error on installation:

"Internal error creating databases. It is possible that you do not have sufficient hard drive space available for the databases."

The details for a workaround in this situation are provided by accessing CSCsb74424 through Bug Toolkit (http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb74424).

System IPCC and Machine Registry Errors

In System IPCC Enterprise, when creating or modifying a machine, if you keep getting the error

"Unable to find the registry on machine XYZ. Make sure the hostname or IP address of the machine is correct, the right IPCC components are installed, and the IPCC Machine Initializer has been run."

and you have double checked everything and re-run the IPCC Machine Initializer on the machine in question, make sure that
"File and Printer Sharing for Microsoft Networks" is turned ON under
Start > Settings > Network Connections... Local Area Connections > General tab > Properties
on that machine.

System IPCC Enterprise Deployment: Restart of Apache Tomcat and Jaguar

When System IPCC Enterprise deployment Machine Initialization is executed, it sets the Apache Tomcat service to automatically run after a reboot. However, in some cases this does not occur. You can then go to Administrator tools in the Start menu and select Services. Select Tomcat and start the service. To get Tomcat to start automatically, take the machine that is running Tomcat out of the domain and then put the machine back into the domain. By doing the above, Tomcat should start automatically. If Tomcat does not start, have your Administrator run netDiag and dcDiag on the machine to verify if the machine is in the domain correctly.

The above discussion applies to the Jaguar service as well.

RMS LGmapper and Operating System Upgrade

Before upgrading the LGMapper server to Windows Server 2003, as a precaution, back up the LGMapper_Alarms and LGArchiver_Alarms. Also, stop and set to manual (or disabled) the LGMapper and LGArchiver services.

RMS Listener Passthru Removed

RMS Listener passthru was never supported in previous RMS/AlarmTracker releases, but appeared in the Listener configuration. The passthru configuration UI has been removed for the RMS 2.1(0) release which supports ICM 7.0(0).

Support for International Character Data

When ICM is installed on localized Windows systems, certain data fields accept native characters while other fields do not. The details of support for international character data in ICM follow:

- Native character data is carried in native language character sets, such as ShiftJIS for Japanese, not Unicode.
- The ICM data fields which support native character data are:
  Agent First Name
  Agent Last Name
  Reason Code Text
  Description fields
  - ICM components such as Configuration Manager will permit entry and display.
  - The VRU interface and CTI Server interface will transport textual data as simple byte strings. There is no guarantee that the string passage will work.

Note Latin1 characters are allowed in English, French, German and Spanish versions of ICM 7.0(0), as well as in English ICM 7.0(0) installed on Latin1 language platforms.

For WebView only, data entry is restricted to ASCII characters.

- Only ASCII characters are accepted for Enterprise names, Call Variables, ECCs, and other fields. If characters other than ASCII are entered, ICM displays an error message. Interface APIs assume ASCII for these data.
- ICM Routing scripts can only be saved using English file names even on localized platforms.

- Multi-media products are expected to conform to ICM data restrictions.

Behavior Change in Node Manager Pending Shutdown / Windows Stopshut

In Windows Server 2003, Microsoft has disallowed local logon once a system shutdown has been initiated. Therefore, an ICM/IPCC Node Manager initiated shutdown can no longer be canceled (via "stopshut" or "shutdown /a") from the local machine unless a user with local administrative privileges is already logged in.

Cancellation of a pending shutdown (including that as initiated by the ICM/IPCC Node Manager) can be achieved by remote invocation from a remote host ("shutdown /a /m" if from Windows Server 2003; syntax varies by Windows operating system) assuming the remote login is properly authenticated as an administrator privileged for the domain.

Conversely, if Support Tools for ICM/IPCC is deployed, the standard tools "stopshut" option may be used to cancel shutdown on the node in question (Support Tools node agent required).

Remote Desktop can also be used to remotely establish a terminal session and issue the stopshut command.

This restriction is specific to the Windows Server 2003 environment and is due to a Microsoft change in local terminal access while a shutdown is pending. See CSCsa39018 for more detail.

UpdateAw Process Fails when domain\username is Greater than 30 Characters

When the domain\username is greater than 30 characters, the CMS node fails with the error: "dis-cms Fail: The domain\username of the current user is longer than the maximum allowed (30 characters)."

Since service logon accounts are always 20 characters in length, a NetBIOS domain name longer than 9 characters will cause this error to occur.

The workaround is to manually shorten the netlogon account name, thus allowing more characters for the NetBIOS domain name.

This can be accomplished using the following steps:

1. On the domain controller, using the Administrative Tool "Active Directory Users and Computers", browse to the ICM instance Organizational Unit.
2. Locate, within the service, logon accounts for the logger and distributor on the system in question.
3. For each, right-click on the account and select "Properties".
4. Select the "Account" tab and shorten the "User logon name (pre-Windows 2000)" field enough so that its length, combined with the domain name, does not exceed 29 characters.

Active Directory Marks ICM Setup Login Users as Invalid, Preventing Login to ICM Setup

On occasion, ICM Setup is unable to login on Loggers and Admin Workstations. The error returned is: error 1057 (The account name is invalid or does not exist, or the password is invalid for the account name specified.).

Due to an unknown network triggering event, Active Directory users for Loggers and AWs (created to logon to the services in the OU) experience a replication issue and are marked as invalid by Active Directory. ICM Setup then creates a new user (instead of replacing the old). When Setup attempts to

login the new user the login fails, because the invalid records persist in the OU and both records have the same name; thus, ICM Setup tries to validate against the invalid record (which has a different password).

This is an Active Directory issue.

To fix this issue, go to Active Directory Users and Computers and drill down through the OU until you get to your instance. Under your instance is where these records are located. Delete the invalid records and rerun Setup.

Cannot Make Configuration Changes because CmsNode Exits Unexpectedly

You may experience a CmsNode shutdown after a buffer overrun is detected. As a result, you cannot make configuration changes using Web Config in System IPCC, nor can you login or make configuration changes through Cisco Collaboration Server or through Cisco E-Mail Manager.

This problem only occurs when the current date/time string (yyyy-m-d-h-m-s) is 19 digits, e.g., 2005-10-10-12-59-99. The problem does not occur when the string is shorter, e.g., 2005-9-30-12-59-99.

To determine if your system is experiencing this problem, examine the cms log on the Distributor AW and search for the error message “Buffer overflow detected”. You can examine a cms log using the following commands from a command prompt.

```
“cdlog <instance name> dis” (where <instance name> is replaced by the name of your
instance)
“dumplog cms /prev”
```

On a Web Config system, any Agent configuration changes such as adding or updating an Agent will fail and produce the error message

```
“Unable to establish connection for update operations”
```

On Cisco Collaboration Server, the Collaboration Server will be unable to connect to the Distributor AW when the CmsNode.exe program is down. This means that any configuration changes, such as adding or editing an agent, will not work. Agents will also be unable to log in through CCS.

To confirm that the connection to the AW is down, perform the following steps:

1. Log into the CCS Admin screen from the CCS server.
2. Select **Collaboration Server > Server Setup > Connection > Monitor**.

With CmsNode down, the Connection Type = “ICM Administrator” row will show a status of “down”. In addition, IIS will not start in a timely fashion and the CCS Admin login will take a long time.

On Cisco E-Mail Manager, you will also be unable to make changes to Agents and Skill groups. For example, attempting to create an agent generates the message

```
**WARN: Create Agent failed with 304 for “<agent name> (-1), Unable to create Agent in ICM
```

For lab environments, you can work around the problem by changing the system date/time so that it is less than 19 digits. For example, setting the date to a month January through September will work around the problem. There is currently no viable workaround for production environments.

For the latest information on this problem, access CSCsc21457 through Bug Toolkit.

ICM Process Dump Behavior Change

Exploiting new Microsoft platform technology, the "Dr. Watson" process failure dump mechanism has been replaced in Release 7.0(0) with Microsoft's "mini-dump" file format. The change should remain largely transparent to customers; however, technical support specialists may encounter ".mdmp" files

over the prior "Dr. Watson" process failure format. The change provides a more efficient means of software error detection and helps to streamline the isolation and remediation of software defects. The information previously found in "Dr. Watson" log files can now be found in the individual ICM log files. In addition to gathering the ICM log files, support personnel should also gather relevant "mini-dump" files found in the individual ICM log file directories.

Customers may also note that new ".pdb" files are present in the ICM bin directory; these are new format symbol files supporting the mini- dump mechanism.

Cannot Replicate Configuration Changes from NAM to CICM

The workaround for this defect (CSCse55800) is provided in Troubleshooting TechNotes
http://www.cisco.com/en/US/partner/products/sw/custcosw/ps5053/products_tech_note09186a00806c6609.shtml

ICM Database Schema Changes, Release 6.0(0) to Release 7.0(0)

This section indicates the changes made to the ICM/IPCC Database Schema between Release 6.0(0) and Release 7.0(0). Refer to the *Database Schema Handbook for Cisco ICM/IPCC Enterprise & Hosted Editions* for descriptions of the new tables and columns.

Tables Added

Machine_Info

Network_Vru_Bank

Tables Added and Reserved for Future Use

Agent_Targeting_Rule

Agent_Targeting_Rule_Member

Agent_Targeting_Rule_Range

Application_Gateway_License

ECC_Payload

ECC_Payload_Member

License_Definition

License_File

License_Real_Time

NIC_Parameter

Tables Deleted

Enterprise_Agent_Group

Enterprise_Agent_Group_Member

Tables Changed

Agent

Columns Added	UserDeletable
Columns Changed	SupervisorAgent, NULL to NOT NULL

Agent_Half_Hour

Columns Added	Reserved 1 – Reserved 5
	RouterCallsAbandQToHalf
	RouterCallsAbandToHalf
	RouterCallsAnsweredToHalf
	RouterCallsDequeuedToHalf
	RouterCallsHandledToHalf
	RouterCallsOfferedToHalf
	RouterCallsRedirectedToHalf
	RouterErrorToHalf
	RouterQCallsToHalf

Agent_Logout

Columns Added	Extension

Agent_Skill_Group_Half_Hour

Columns Added	AbandonHoldOutCallsToHalf
	NetConfOutCallsTimeToHalf
	NetConferencedOutCallsToHalf
	NetConsultativeCallsTimeToHalf
	NetConsultativeCallsToHalf
	NetTransferredOutCallsToHalf
	Reserved 1 – Reserved 5

AWControl

Columns Added	ConfigChangedByUserName, VNAME32 to VARCHAR(64)

Call_Type_Half_Hour

Columns Added	AgentErrorCountToHalf
	CallDelayAbandTimeToHalf
	CallsRequeriedToHalf
	CTDelayAbandTimeToHalf
	CTVRUTimeToHalf
	DelayAgentAbandTimeToHalf
	RouterCallsAbandToAgentToHalf
	ServiceLevelErrorToHalf
	ServiceLevelRONAToHalf
	TotalCallsAbandToHalf
	VRUTimeToHalf

NOTE

For customers who are migrating from Release 6.0(0) to Release 7.0(0), the data stored in DelayQAbandTimeHalf and RouterCallsAbandQToHalf has been moved to TotalCallsAbandToHalf and CallDelayAbandTimeToHalf respectively.

The database field Call_Type_Half_Hour.RouterCallsAbandQToHalf prior to 7.0(0) included the count for all calls that abandoned for the call type and Call_Type_Half_Hour.DelayQAbandTimeHalf included the time associated with these abandon calls.

In Release 7.0(0) these fields only include calls that abandoned in queue. New database fields have been added to the Call_Type_Half_Hour table that provide breakout of different abandons for Call Type. Fields added provide abandon counts and the time associated with these abandons. The different abandons are as follows:

- Calls that abandon in queue (RouterCallsAbandQToHalf and DelayQAbandTimeHalf)
- Calls that abandon at the agent desktop before being answered (RouterCallsAbandToAgentToHalf and DelayAgentAbandTimeToHalf)
- Count of all abandons, this also includes calls that abandon prior to queuing. (TotalCallsAbandToHalf and CallDelayAbandTimeToHalf)

For more information, refer to the *Database Schema Handbook for Cisco ICM/IPCC Enterprise & Hosted Editions*.

Call_Type_Real_Time

Columns Added	AgentErrorCountHalf
	AgentErrorCountToday
	CallDelayAbandTimeHalf
	CallDelayAbandTimeTo5
	CallDelayAbandTimeToday
	CallsAtAgentNow
	CallsAtVRUNow
	CTDelayAbandTimeHalf
	CTDelayAbandTimeTo5
	CTDelayAbandTimeToday
	DelayAgentAbandTimeHalf
	DelayAgentAbandTimeTo5
	DelayAgentAbandTimeToday
	RouterCallsAbandToAgentHalf
	RouterCallsAbandToAgentTo5
	RouterCallsAbandToAgentToday
	ServiceLevelErrorHalf
	ServiceLevelErrorToday
	ServiceLevelRONAHalf
	ServiceLevelRONATO5
	ServiceLevelRONAToday
	TotalCallsAbandHalf
	TotalCallsAbandTo5
	TotalCallsAbandToday

Campaign

Columns Added	AbandonCustomerCallback
	AbandonedDialerCallback

	AnsweringMachineCallback
	CustomerNotHomeCallback
	DisableCPA
	DSTLocation
	PrefixDigits
	WaitForBusyRetry

Campaign_Query_Rule_Half_Hour

Columns Added	CallbackCountToHalf
	CustomerNotHomeCountToHalf
	PersonalCallbackCountToHalf
	WrongNumberCountToHalf

Campaign_Query_Rule_Real_Time

Columns Added	CustomerNotHomeCount
	PersonalCallbackCount
	WrongNumberCount

Campaign_Skill_Group

Columns Added	DialedNumber
Columns Deleted	SkillTargetIDPredictive
	SkillTargetIDPreview

Campaign_Target_Sequence

Columns Added	PhoneIndex
	ZoneIndex
Columns Deleted	RangeType
	TargetType

Cfg_Mngr_User_Desktop_Snap

Columns Changed	DesktopSnapShotName, VNAME32 to VARCHAR(128)

Cfg_Mngr_User_Settings

Columns Changed	LoginName, VARCHAR(100) to NOT VARCHAR(128)

Class_Security

Columns Changed	UserGroupName, VARCHAR(30) to VARCHAR(64)

Dialed_Number

Columns Added	PermitApplicationRouting
	ReservedByIVR

Dialer

Columns Added	IPBridgingEnabled

Dialer_Half_Hour

Columns Added	CallbackCountToHalf
	CustomerNotHomeCountToHalf
	PersonalCallbackCountToHalf
	WrongNumberCountToHalf

Dialer_Real_Time

Columns Added	AbandonToIVRHalf
	AgentClosedDetectHalf
	AgentRejectedDetectHalf
	CallbackCount
	CancelledDetectHalf
	CustomerAbandonDetectHalf
	CustomerNotHomeCount
	FaxDetectHalf
	NetworkAnsMachineDetectHalf
	NoDialToneDetectHalf
	NoRingBackDetectHalf

	PersonalCallbackCount
	WrongNumberCount

Expanded_Call_Variable

Columns Added	Persistent

Group_Security_Control

Columns Changed	UserGroupName, VARCHAR(30) to VARCHAR (64)

ICR_Globals

Columns Added	ExternalScriptValidation
	IPCCDeploymentType
	IPCCDeploymentState
Columns Changed	CCDomainName, VNAME(32) to VARCHAR (64)

ICR_Locks

Columns Changed	UserName, VNAME (32) to VARCHAR (64)

ICR_Node

Columns Changed	DomainName, VNAME (32) to VARCHAR (64)

Logical_Interface_Controller

Columns Changed	Deleted, NULL to NOT NUL

Object_Security

Columns Changed	UserGroupName, VARCHAR (30) to VARCHAR (64)

Peripheral

Columns Added	AgentTargetingMethod
	InternalIPTAOnly
	AgentTargetingMethod

Columns Changed	AgentAutoConfig, NULL to NOT NULL
	AgentReporting, NULL to NOT NULL

Recurring_Schedule_Map

Columns Changed	Bool1, NULL to NOT NULL
	Bool2, NULL to NOT NULL

Region_Prefix

Columns Added	DaylightSavingsEnabled
Columns Deleted	DaylightSavingsStart
	DaylightSavingsEnd

Route_Call_Detail

Columns Added	MRDomainID

Route_Half_Hour

Columns Added	RedirectNoAnsCallsToHalf
RedirectNoAnsCallsToHalf	Reserved1 - Reserved5
Columns Changed	TimeZone, NULL to NOT NULL

Route_Real_Time

Columns Added	RedirectNoAnsCallsTo5
	RedirectNoAnsCallsHalf
	RedirectNoAnsCallsToday

Routing_Client_Five_Minute

Columns Added	NumConsultConfTo5
	NumCallHeldEventTo5
	NumCallOriginatedEventTo5
	NumCallEstablishedEventTo5
	NumRetrievedEventTo5

	NumConnectionClearedEventTo5
	NumConferencedEventTo5
	NumAlternateCallReqTo5
	NumAlternateCallConfTo5
	NumReconnectCallReqTo5
	NumReconnectCallConfTo5
	NumConsultTransferReqTo5
	NumConsultTransferConfTo5
	NumConferenceCallReqTo5
	NumConferenceCallConfTo5
	NumDropConnectionReqTo5
	NumDropConnectionConfTo5

Schedule_Import

Columns Changed	Bool1, NULL to NOT NULL
	Bool2, NULL to NOT NULL

Sec_Group

Columns Changed	UserGroupName, VARCHAR (30) toVARCHAR(64)

Sec_User

Columns Changed	UserGroupName, VARCHAR (30) to VARCHAR (64)

Service

Columns Added	UserDeletable

Service_Half_Hour

Columns Added	RedirectNoAnsCallsToHalf
	Reserved1 - Reserved5

Service_Real_Time

Columns Added	RedirectNoAnsCallsTo5
	RedirectNoAnsCallsHalf
	RedirectNoAnsCallsToday

Skill_Group

Columns Added	ServiceThreshold
	ServiceType
	UserDeletable

Skill_Group_Half_Hour

Columns Added	AbandoHoldCallsOutToHalf
	NetConsultativeCallsToHalf
	NetConsultativeCallsTimeToHalf
	NetConferencedOutCallsToHalf
	NetConfOutCallsTimeToHalf
	NetTransferOutCallsToHalf
	RouterCallsOfferedToHalf
	RouterCallsAbandToAgentToHalf
	RouterCallsDequeuedToHalf
	RouterErrorToHalf
	ServiceLevelToHalf
	ServiceLevelCallsToHalf
	ServiceLevelCallsAbandToHalf
	ServiceLevelCallsDequeueToHalf
	ServiceLevelErrorToHalf
	ServiceLevelRONAToHalf
	ServiceLevelCallsOfferedToHalf
	Reserved1 - Reserved5

Skill_Group_Real_Time

Columns Added	RouterCallsAbandQTo5
	RedirectNoAnsCallsTo5
	RouterCallsAbandToAgentTo5
	RouterCallsDequeuedTo5
	RouterCallsOfferedTo5
	ServiceLevelCallsAbandTo5
	ServiceLevelCallsDequeuedTo5
	ServiceLevelCallsOfferedTo5
	ServiceLevelCallsTo5
	ServiceLevelTo5
	ServiceLevelRONATo5

User_Group

Columns Added	UserGuid
	UserName
	DomainName
Columns Changed	UserGroupName, VARCHAR (30) to VARCHAR (64)

User_Group_Member

Columns Changed	UserGroupName, VARCHAR (30) to VARCHAR (64)
	UserName, VARCHAR (30) to VARCHAR (64)

User_Security_Control

Columns Changed	UserName, VARCHAR(30) to VARCHAR(64)

Version

Columns Added	IPCCMinor

ICM Database Schema Changes, Release 5.0(0) to Release 7.0(0)

Since Release 6.0(0) was an Enterprise Edition release only, for the convenience of Hosted Edition customers, this section indicates the changes made to the ICM/IPCC Database Schema between Release 5.0(0) and Release 7.0(0). Refer to the *Database Schema Handbook for Cisco ICM/IPCC Enterprise & Hosted Editions* for descriptions of the new tables and columns.

Tables Added

- Agent_Event_Detail
- Bucket Intervals

  Note that for the Bucket_Intervals table, a default record is created with following data:

Column	Value
BucketIntervalID	1
EnterpriseName	Default_Bucket_Intervals
IntervalUpperBound1	8
IntervalUpperBound2	30
IntervalUpperBound3	60
IntervalUpperBound4	90
IntervalUpperBound5	120
IntervalUpperBound6	180
IntervalUpperBound7	300
IntervalUpperBound8	600
IntervalUpperBound9	1200

- Machine_Info
- Reason_Code
- Network_Vru_Bank

Tables Added and Reserved for Future Use

- Agent_Targeting_Rule
- Agent_Targeting_Rule_Member
- Agent_Targeting_Rule_Range
- Application_Gateway_License
- ECC_Payload
- ECC_Payload_Member
- License_Definition
- License_File
- License_Real_Time
- NIC_Parameter

Tables Deleted

- Enterprise_Agent_Group
- Enterprise_Agent_Group_Member

Index Added

As noted in the table changes in the pages that follow, DbDateTime is now an additional index in the following tables:

- Agent_Event_Detail
- Agent_Half_Hour
- Agent_Skill_Group_Half_Hour
- Application_Gateway_Half_Hour
- Call_Type_Half_Hour
- Campaign_Query_Rule_Half_Hour
- Dialer_Half_Hour
- Network_Trunk_Group_Half_Hour
- Peripheral_Half_Hour
- Physical_Controller_Half_Hour
- Route_Call_Detail
- Route_Call_Variable
- Route_Half_Hour
- Service_Half_Hour
- Skill_Group_Half_Hour
- Termination_Call_Detail
- Termination_Call_Variable
- Trunk_Group_Half_Hour

Tables Changed

Agent

Columns Added	UserDeletable
Columns Changed	SupervisorAgent, NULL to NOT NULL

Agent_Half_Hour

Columns Added	DbDateTime Reserved 1 – Reserved 5 RouterCallsAbandQToHalf RouterCallsAbandToHalf RouterCallsAnsweredToHalf RouterCallsDequeuedToHalf RouterCallsHandledToHalf RouterCallsOfferedToHalf RouterCallsRedirectedToHalf RouterErrorToHalf RouterQCallsToHalf

Agent_Logout

Columns Added	Extension

Agent_Real_Time

Columns Added	RouterCallsQueueNow RouterLongestCallQ

Agent_Skill_Group_Half_Hour

Columns Added	AbandonHoldOutCallsToHalf DbDateTime NetConfOutCallsTimeToHalf NetConferencedOutCallsToHalf NetConsultativeCallsToHalf NetConsultativeCallsTimeToHalf NetTransferredOutCallsToHalf Reserved 1 – Reserved 5

Application_Gateway_Half_Hour

Columns Added	DbDateTime

AWControl

Columns Added	ConfigChangedByUserName, VNAME32 to VARCHAR(64)

Blended_Agent_Option

Columns Added	IPDirectDialPreview

Call_Type

Columns Added	BucketIntervalID

Call_Type_Half_Hour

Columns Added	AbandInterval1 AbandInterval2 AbandInterval3 AbandInterval4 AbandInterval5 AbandInterval6 AbandInterval7 AbandInterval8 AbandInterval9 AbandInterval10 AgentErrorCountToHalf AnsInterval1 AnsInterval2 AnsInterval3 AnsInterval4 AnsInterval5 AnsInterval6 AnsInterval7 AnsInterval8 AnsInterval9 AnsInterval10 BucketIntervalID CallsAnsweredToHalf CallDelayAbandTimeToHalf CallsRequeriedToHalf CallsRoutedNonAgentToHalf CallsRONAToHalf CallsQHandledToHalf CTDelayAbandTimeToHalf CTVRUTimeToHalf DelayAgentAbandTimeToHalf DbDateTime ReturnReleaseToHalf RouterCallsAbandToAgentToHalf ServiceLevelErrorToHalf

Call_Type_Half_Hour Colums Added cont.	ServiceLevelRONAToHalf ServiceLevelType TotalCallsAbandToHalf VRUAssistedCallsToHalf VRUForcedXferredCallsToHalf VRUHandledCallsToHalf VRUOptOutUnhandledCallsToHalf VRUOtherCallsToHalf VRUScriptedXferredCallsToHalf VRUTimeToHalf VRUUnhandledCallsToHalf

NOTE

In Release 7.0(0), the data stored in DelayQAbandTimeHalf and RouterCallsAbandQToHalf has been moved to TotalCallsAbandToHalf and CallDelayAbandTimeToHalf respectively.

The database field Call_Type_Half_Hour.RouterCallsAbandQToHalf prior to 7.0(0) included the count for all calls that abandoned for the call type and Call_Type_Half_Hour.DelayQAbandTimeHalf included the time associated with these abandon calls.

In Release 7.0(0) these fields only include calls that abandoned in queue. New database fields have been added to the Call_Type_Half_Hour table that provide breakout of different abandons for Call Type. Fields added provide abandon counts and the time associated with these abandons. The different abandons are as follows:

- Calls that abandon in queue (RouterCallsAbandQToHalf and DelayQAbandTimeHalf)
- Calls that abandon at the agent desktop before being answered (RouterCallsAbandToAgentToHalf and DelayAgentAbandTimeToHalf)
- Count of all abandons, this also includes calls that abandon prior to queuing. (TotalCallsAbandToHalf and CallDelayAbandTimeToHalf)

For more information, refer to the *Database Schema Handbook for Cisco ICM/IPCC Enterprise & Hosted Editions*.

Call_Type_Real_Time

Columns Added	AgentErrorCountHalf AgentErrorCountToday CallDelayAbandTimeHalf CallDelayAbandTimeTo5 CallDelayAbandTimeToday CallsAnsweredTo5 CallsAnsweredHalf CallsAnsweredToday CallsAtAgentNow CallsRONATo5 CallsRONAHalf CallsRONAToday CallsRoutedNonAgentHalf CallsRoutedNonAgentToday CallsRoutedNonAgentTo5 CallsAtVRUNow CTDelayAbandTimeHalf CTDelayAbandTimeTo5 CTDelayAbandTimeToday DelayAgentAbandTimeHalf DelayAgentAbandTimeTo5 DelayAgentAbandTimeToday ReturnReleaseHalf ReturnReleaseToday RouterCallsAbandToAgentHalf RouterCallsAbandToAgentTo5 RouterCallsAbandToAgentToday ServiceLevelErrorHalf ServiceLevelErrorToday ServiceLevelRONAHalf ServiceLevelRONATo5 ServiceLevelRONAToday TotalCallsAbandHalf TotalCallsAbandTo5 TotalCallsAbandToday

Campaign

Columns Added	AbandonCustomerCallback AbandonedDialerCallback AMDTreatmentMode AnsweringMachineCallback CampaignPurposeType ConfigParam CustomerNotHomeCallback DisableCPA DSTLocation IPAMDEnabled IPTerminatingBeepDetect PrefixDigits UseGMTFromRegionPrefix WaitForBusyRetry
Columns Deleted	ACDMessageQueue

Campaign_Query_Rule_Half_Hour

Columns Added	AbandonDetectToHalf AbandonToIVRToHalfHour AgentClosedDetectToHalf AgentRejectedDetectToHalf AnsweringMachineDetectToHalf BusyDetectToHalf CallbackCountToHalf CancelledDetectToHalf CustomerAbandonDetectToHalf CustomerNotHomeCountToHalf DbDateTime FaxDetectToHalf NetworkAnsMachineDetectToHalf NoAnswerDetectToHalf NoDialToneDetectToHalf NoRingBackDetectToHalf PersonalCallbackCountToHalf WrongNumberCountToHalf SITToneDetectToHalf
Columns Renamed	AttemptedToHalf to ContactsAttemptedToHalf ContactedToHalf to VoiceDetectToHalf

Campaign_Query_Rule_Real_Time

Columns Added	AbandonDetectCount AbandonToIVRCount AgentClosedCount AgentRejectedCount AnsweringMachineCount CancelledDetectCount CustomerAbandonedDetectCount CustomerNotHomeCount FaxDetectCount NetworkAnsMachineCount NoAnswerDetectCount NoDialToneDetectCount NoRingBackDetectCount PersonalCallbackCount SITToneDetectCount
Columns Renamed	ContactedCount to VoiceCount

Campaign_Skill_Group

Columns Added	AbandonedRoutePoint ConfigParam DialedNumber IVRPorts IVRRoutePoint
Columns Deleted	SkillTargetIDPredictive SkillTargetIDPreview

Campaign_Target_Sequence

Columns Added	ConfigParam PhoneIndex ZoneIndex
Columns Deleted	RangeType TargetType

Cfg_Mngr_User_Desktop_Snap

Columns Changed	DesktopSnapShotName, VNAME32 to VARCHAR(128)

Cfg_Mngr_User_Settings

Columns Changed	LoginName, VARCHAR(100) to NOT VARCHAR(128)

Class_Security

Columns Changed	UserGroupName, VARCHAR(30) to VARCHAR(64)

Dialed_Number

Columns Added	PermitApplicationRouting ReservedByIVR

Dialer

Columns Added	ConfigParam IPBridgingEnabled LongDistancePrefix
Columns Changed	LocalAreaCode – type Varchar(100), Null

Dialer_Half_Hour

Columns Added	AbandonToIVRToHalf AgentClosedDetectToHalf AgentRejectedDetectToHalf CallbackCountToHalf CancelledDetectToHalf CustomerAbandonDetectToHalf CustomerNotHomeCountToHalf DbDateTime FaxDetectToHalf NetworkAnsMachineDetectToHalf NoDialToneDetectToHalf NoRingBackDetectToHalf PersonalCallbackCountToHalf WrongNumberCountToHalf

Dialer_Real_Time

Columns Added	AbandonToIVRHalf AgentClosedDetectHalf AgentRejectedDetectHalf CallbackCount CancelledDetectHalf CustomerAbandonDetectHalf CustomerNotHomeCount FaxDetectHalf NetworkAnsMachineDetectHalf NoDialToneDetectHalf NoRingBackDetectHalf PersonalCallbackCount WrongNumberCount

Expanded_Call_Variable

Columns Added	Persistent

Group_Security_Control

Columns Changed	UserGroupName, VARCHAR(30) to VARCHAR (64)

ICR_Globals

Columns Added	BucketIntervalID ExternalScriptValidation IPCCDeploymentType IPCCDeploymentState
Columns Changed	CCDomainName, VNAME(32) to VARCHAR (64)

ICR_Locks

Columns Changed	UserName, VNAME (32) to VARCHAR (64)

ICR_Node

Columns Changed	DomainName, VNAME (32) to VARCHAR (64)

Logical_Interface_Controller

Columns Changed	Deleted, NULL to NOT NUL

Network_Trunk_Group_Half_Hour

Columns Added	DbDateTime

Object_Security

Columns Changed	UserGroupName, VARCHAR (30) to VARCHAR (64)

Peripheral

Columns Added	AgentEventDetail AgentTargetingMethod InternalIPTAOnly
Columns Changed	AgentAutoConfig, NULL to NOT NULL AgentReporting, NULL to NOT NULL

Peripheral_Half_Hour

Columns Added	DbDateTime MaxCallsInProgress NumberofSamples ServiceLevelType TotalCallsInProgressSamples

Physical_Controller_Half_Hour

Columns Added	DbDateTime

Recurring_Schedule_Map

Columns Changed	Bool1, NULL to NOT NULL Bool2, NULL to NOT NULL

Region_Prefix

Columns Added	DaylightSavingsEnabled
Columns Deleted	DaylightSavingsEnd DaylightSavingsStart

Route_Call_Detail

Columns Added	BeganCallTypeDateTime BeganRoutingDateTime DbDateTime MRDomainID RequeryResult TargetType VRUProgress

Route_Call_Variable

Columns Added	DbDateTime

Route_Half_Hour

Columns Added	DbDateTime RedirectNoAnsCallsToHalf Reserved1 - Reserved5 ServiceLevelType
Columns Changed	TimeZone, NULL to NOT NULL

Route_Real_Time

Columns Added	RedirectNoAnsCallsTo5 RedirectNoAnsCallsHalf RedirectNoAnsCallsToday

Routing_Client_Five_Minute

Columns Added	NumConsultConfTo5 NumCallHeldEventTo5 NumCallOriginatedEventTo5 NumCallEstablishedEventTo5 NumRetrievedEventTo5 NumConnectionClearedEventTo5 NumConferencedEventTo5 NumAlternateCallReqTo5 NumAlternateCallConfTo5 NumReconnectCallReqTo5 NumReconnectCallConfTo5 NumConsultTransferReqTo5 NumConsultTransferConfTo5 NumConferenceCallReqTo5 NumConferenceCallConfTo5 NumDropConnectionReqTo5 NumDropConnectionConfTo5

Schedule_Import

Columns Changed	Bool1, NULL to NOT NULL Bool2, NULL to NOT NULL

Sec_Group

Columns Changed	UserGroupName, VARCHAR (30) toVARCHAR(64)

Sec_User

Columns Changed	UserGroupName, VARCHAR (30) to VARCHAR (64)

Service

Columns Added	UserDeletable

Service_Half_Hour

Columns Added	DbDateTime RedirectNoAnsCallsToHalf Reserved1 - Reserved5

Service_Real_Time

Columns Added	RedirectNoAnsCallsTo5 RedirectNoAnsCallsHalf RedirectNoAnsCallsToday

Skill_Group

Columns Added	ServiceThreshold ServiceType UserDeletable

Skill_Group_Half_Hour

Columns Added	AbandoHoldCallsOutToHalf DbDateTime NetConsultativeCallsToHalf NetConsultativeCallsTimeToHalf NetConferencedOutCallsToHalf NetConfOutCallsTimeToHalf NetTransferOutCallsToHalf RouterCallsOfferedToHalf RouterCallsAbandToAgentToHalf RouterCallsDequeuedToHalf RouterErrorToHalf ServiceLevelToHalf ServiceLevelCallsToHalf ServiceLevelCallsAbandToHalf ServiceLevelCallsDequeueToHalf ServiceLevelErrorToHalf ServiceLevelRONAToHalf ServiceLevelCallsOfferedToHalf Reserved1 - Reserved5

Skill_Group_Real_Time

Columns Added	RouterCallsAbandQTo5 RedirectNoAnsCallsTo5 RouterCallsAbandToAgentTo5 RouterCallsDequeuedTo5 RouterCallsOfferedTo5 ServiceLevelCallsAbandTo5 ServiceLevelCallsDequeuedTo5 ServiceLevelCallsOfferedTo5 ServiceLevelCallsTo5 ServiceLevelTo5 ServiceLevelRONATo5

Termination_Call_Detail

Columns Added	DbDateTime NetQTime

Termination_Call_Variable

Columns Added	DbDateTime

Trunk_Group_Half_Hour

Columns Added	DbDateTime

User_Group

Columns Added	DomainName UserGuid UserName
Columns Changed	UserGroupName, VARCHAR (30) to VARCHAR (64)

User_Group_Member

Columns Changed	UserGroupName, VARCHAR(30) to VARCHAR(64) UserName, VARCHAR (30) to VARCHAR (64)

User_Security_Control

Columns Changed	UserName, VARCHAR(30) to VARCHAR(64)

Version

Columns Added	IPCCMinor

User Documentation Updates

This section discusses changes and additions to the ICM/IPPC Enterprise and Hosted Editions software documentation set.

Documentation Changes

- The style of the manual titles has changed to more immediately indicate the content of the manual, as well as to more completely indicate the products for which the document is of interest. For example, what was formerly titled the *Cisco ICM/IP Contact Center Enterprise Edition Database Schema Handbook* is now titled the *Database Schema Handbook for Cisco ICM/IPCC Enterprise & Hosted Editions*.
- *SNMP Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*—a new document that provides information on Simple Network Management Protocol (SNMP) basics, installation prerequisites, configuration, MIB (Management Information Base) support, and troubleshooting for ICM/IPCC SNMP support.
- *Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*—with Release 7.0(0) taking fuller advantage of Active Directory than previous releases, it is essential that this document be consulted before attempting to install ICM/IPCC 7.0(0).
- *ICM Upgrade Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*—this document has been rewritten to include more detailed upgrade procedures, and includes upgrade checklists to make it easier to keep track of progress during a system upgrade; be especially sure to follow the procedures presented in this guide as the upgrade process for Release 7.0(0) is substantially different from the upgrade process in previous releases.
- *System IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition*—a new document that provides information to help you understand, install, and configure the System deployment of IPCC Enterprise.
- *IPCC Gateway Deployment Guide*—a new document that provides information on implementing IPCC Gateway, a feature that allows IPCC Enterprise or IPCC Express to act as traditional or enhanced ACDs connected to ICM.
- *WebView Template Reference Guide for Cisco IPCC Enterprise & Hosted Editions*—this document has been enhanced by the addition of screen shots for many of the most commonly used templates.
- *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification*—the document initially entitled, and referred to in the Release 7.0(0) documentation set as, the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials* has been retitled the *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification* to better indicate its contents.

Clarification on Some Agent_Skill_Group_Half_Hour and Skill_Group_Half_Hour Fields

In the Schema documentation for the Agent_Skill_Group_Half_Hour and Skill_Group_Half_Hour tables should be noted:

Because of rounding, the formula provided for LoggedOnTimeToHalf is not accurate. Ignore the formula.

Because of rounding, the various time element data such as AgentOutCallsTimeToHalf, HoldTimeToHalf, LoggedOnTimeToHalf (and so on) in the Agent_Skill_Group_Half_Hour table may differ slightly from the comparable data in the Skill_Group_Half_Hour table. The data in the latter are more exact.

Network Consultative Transfer Limited to 3-party Conference

The following discussion should be included in the *Product Description Guide for Cisco ICM Hosted Edition*.

Network Consultative Transfer (NCT), as the name implies, is intended primarily for one agent to consult with a second agent before transferring a call to the second agent.

However, with limitations, NCT can also be used for conferencing.

4-party network conferences are not directly supported. A party in a 3-party conference that has initiated a Network Consultative Transfer (NCT), can **not** initiate another NCT.

For example:

1. Caller calls Agent 1.
2. Agent 1 answers the call.
3. Agent 1 initiates NCT to Agent 2.
4. Agent 2 answers the call.
5. Agent 1 completes the conference.
6. Caller, Agent 1 and Agent 2 are in conference.
7. Agent 1 cannot initiate another NCT to another agent.

However:

8. Agent 2 can initiate NCT to Agent 3.

Thus, although Agent 1's desktop would show a 3-party conference, and Agent 2's desktop would show a 3-party conference, there would be—in effect—a 4-party conference.

CallsAnsweredToHalf Does Not Include InternalCallsReceivedToHalf

In the *Database Schema Handbook*, in tables Agent_Skill_Group_Half_Hour and Skill_Group_Half_Hour, it is stated in the description for the field CallsAnsweredToHalf that the value for this field includes internal calls (InternalCallsReceivedToHalf). This is not true. Only inbound calls are counted.

Security Best Practices Guide and Windows OS Support

For the currently supported Windows operating system software, see the latest *Hardware and System Software Specification (Bill of Materials) for Cisco ICM/IPCC Enterprise and Hosted Editions*, not the *Security Best Practices Guide*.

ICM-to-ICM Gateway User Guide

With the Release 7.0(0) support for Active Directory, the section “Configuring ICM Instances on the Client ICM”, in Chapter 2 of the *ICM-to-ICM Gateway User Guide*, has become unnecessary. Indeed, attempting to use it can result in difficulties. This section should be **ignored**.

Configuration Parameters for Routing Client on INCRP NIC

In Step 10 of the "How to define the INCRP NIC" subsection, in Chapter 3 of the *Setup and Configuration Guide for Cisco ICM Hosted Edition*, the following statement is made:

If your NAM has multiple routing clients, ensure that each client is defined and that the ClientType field in the Routing Client record matches the client type of the NAM's NIC. In addition, the Configuration Parameter field for each record must contain the parameter

/CustomerID <RCID>

where <RCID> is the Routing Client ID of the matching routing client on the NAM, as defined in the SQL table.

In fact, the /ssn switch is functionally equivalent to the /CustomerID switch.

Note You **cannot** (nor do you need to) use both in the same configuration line, since one will override the other.

The "/CustomerID xxxx" configuration parameter is (by convention) used to map the remote NAM Routing Client xxxx with the local CICM Routing Client. (As stated, this is just a convention. If existing customers are using "/ssn xxxx", where xxx is the Remote RCID, they have a functional configuration.)

An example would be a NAM-CICM system where the NAM has an Ss7InNic out to the carrier network. On the CICM, the INCRPNIC Routing Client (routing to the Ss7InNic) would have the configuration parameter "/CustomerID xxxx" where xxxx is the Ss7InNic's Routing Client ID on the NAM. On the NAM, the SS7InNic Routing Client may have an /ssn configuration parameter.

Outbound Option: CallsMadeToZone

In the *Outbound Option User Guide*, in the section “Dialing List Table Columns”, it is stated that

- CallsMadeToZone1 contains as its value “The number of calls made to numbers in zone 1.”
- CallsMadeToZone2 contains as its value “The number of calls made to numbers in zone 2.”

This is somewhat misleading. The Dialing List Table is used by CampaignManager to determine what to do next. Therefore, for a call which Outbound Agent has scheduled a callback, the CallResult will be set to Voice Callback(14), but CallsMadeToZone1 or CallsMadeToZone2 will be reset to 0.

Service Level and Services Auto-Configured in a Unified ICME Parent/Unified CCX Child Model

In the *Cisco IPCC Gateway Deployment Guide for Unified ICME, Unified CCE, and Unified CCX* manual, the section “Understanding Reporting in the Unified ICME Parent and Unified CCX Child Deployment Model” contains the following:

Difference in Service Level Concept Implementation. Service Level for Unified ICME is calculated for Services, not Skill Groups. Service Level in Unified CCX is calculated for CSQs (which correspond to Unified ICME Skill Groups), not Applications (which correspond to Unified ICME Services). Since values are not being calculated on equivalent objects, a Unified CCX Service Level report is not comparable to a Unified ICME Service Level report.

The above might be interpreted to mean that Service Level is calculated and available for the Services auto-configured in a Unified ICME Parent/Unified CCX Child deployment model. This is not the case.

It is not possible to define Service Levels for Services auto-configured in a Unified ICME Parent/Unified CCX Child environment. Instead, an option is to have all calls translation-routed to the Child and use CallType reports on the Parent to access Service Level information at the Enterprise level.

Configuration Group Users and Configuration Tools

If the configuration group in the domain was deleted and recreated after the distributor installation, a User in the configuration group may be unable to start configuration tools. The user receives an error indicating that a connection to the database could not be opened. The distributor service updateaw process will not start because it fails to connect to the logger database.

The Domain Manager may be used to repair the organizational unit structure, such that the groups are recreated. When Active Directory groups are recreated with the same name, the group is not actually identical. In this case, SQL is giving configuration and service permissions to the deleted group instead of to the new group. To determine if the group SQL is giving permission to has been deleted use Query Analyzer to execute the command "sp_validatelogins"

If the command indicates that the configuration or service group is no longer a valid login, then the login and associated users must be removed. Use SQL Enterprise Manager to remove the invalid users from the logger and AW databases, and remove the logins. After the logins have been removed, run local setup and edit the Logger and Distributor components. This will cause the logins to be recreated using the correct domain group.

Running Internet Script Editor

If the file dbagent.acl does not exist, Setup creates the file and gives full read/write access to this file to every user logged onto the system.

It is the CallRouter that accesses the file to read and write, so the file access should be with read/write access.

If the user changes the attribute of this file by not giving read/write access to the users, then it will cause applications like Internet Script Editor (ISE) to fail.

In such a case, an attempt to start ISE results in the following error appearing in iseman log:
"GetLock: lock denied/insufficient permission".
In the dbagent log, the error message is:
"Unable to access dbagent.acl during security check".

As already indicated, this is because the ISE user does not have access to the icm\<inst>\ra\dbagent.acl file on the CallRouter.

ISE users must have full access to the dbagent.acl file on the CallRouter.

Peripheral Gateway Failover

The “Peripheral Gateways” section of the “Fault Tolerance” chapter in the *ICM Administration Guide* should contain the following Note:

Note In ICM Enterprise, as a default, OPC does not keep calls in memory waiting to be re-initialized upon PIM activation after a PG failover. This might result in calls having calltype, call variables and ECC variables lost on Agent Desktops when a PG failover occurs.

Important Notes

The following sections contain restrictions that apply to Release 7.0(0).

Note Limitations ("no more than n connections can be made to ...") and scalability ("up to x agents can ...") are discussed in the *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)*.

Time Zone and Daylight Savings Time Updates

Many Cisco contact center products and/or components use Java technology in their implementation. For each server upon which Java-based components are installed, the appropriate Java Runtime Environment (JRE) or Java Development Kit (JDK) is also installed during the product installation process. Due to a plethora of worldwide changes to time zones, daylight savings time implementation changes including start/stop dates and times (and many done with very little advance warning), it is difficult for Cisco to keep pace with changes and provide patches and/or guidance for compliance. It is therefore suggested that after the installation/upgrade of any of the products listed below, the person who performed the installation/upgrade should download and apply the latest version of the Sun JDK DST Timezone Update Tool — TZUpdater — to each server on which each of these Java-based products are installed.

- WebView Enterprise Reporting
- System IPCC / SCCE Web Administration
- Configuration Management Service (CMS) (if enabled on the Admin Workstation)
- System IPCC / CCE Agent Reskilling Web Tool
- IPCC / CCE (CallManager) Peripheral Gateway (JTAPI Gateway)
- CTI Toolkit Java Integration Library API (JavaCIL)
- Email Interaction Manager (EIM)
- Web Interaction Manager (WIM)
- Contact Center Management Portal (CCMP)
- Cisco Agent Desktop (CAD) Enterprise Service
- CAD-BE
- IP Phone Agent

CallManager 4.x Consideration for External Calls in IPCC Enterprise

In CallManager 4.x, there is an issue where overlap sending is disabled by default in the CallManager gateway configuration. If overlap sending is disabled, this causes external calls to be counted as internal calls in IPCC Enterprise. When the overlap sending is re-enabled, the IPCC Enterprise reporting is correct for external calls.

Note This condition is limited to CallManager 4.x. It is not a consideration for CallManager 5.x and later.

To restate this slightly:

When an agent makes an external call, IPCC Enterprise reporting depends on network Events to correctly classify the call type. When deploying IPCC Enterprise with CallManager 4.x, the network Events will not be available with the default CallManager 4.x configuration.

There are two alternative ways to enable network Events.

- Enable overlap sending by setting it on in the CallManager gateway configuration. This is off by default.
- Change the jtapi.ini file on the PG system.

To change the jtapi.ini file:

Step 1 Go to
c:\windows\java\lib
or
c:\winnt\java\lib
(depending on the version of the Windows operating system)

Step 2 From the IPCC PG, access a command prompt and enter
java CiscoJtapiVersion -parms > Jtapi.ini

Step 3 Open the jtapi.ini file in a text editor.

Step 4 Add this line:
AllowNetworkEventsAfterOffered=1
or change the line to
AllowNetworkEventsAfterOffered=1

Step 5 Save and close the file.

Step 6 Recycle the PG service.

Manual Intervention to Restart ICM Processes after an Exception

Sometimes, manual intervention is required to restart ICM Processes after an exception. This error can be suppressed by setting a registry value.

If you want to suppress the Windows exception, The following must be done:

Set the registry key value to 2 for the registry key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows\ErrorMode".

For more information, please refer to link: http://support.microsoft.com/kb/128642

Remote Desktop Not Supported for Installation

Remote Desktop must not be used to install ICM Enterprise, ICM Hosted, IPCC Enterprise, IPCC Hosted.

Remote Desktop can be used for remote administration.

User Variable Name Restriction

Beginning with Release 7.0(0), User Variable names must not contain a period/dot (.).

Replicating Configuration Changes from NAM to CICM & NAM to NAM

Setup for ICM 7.0(0), and later versions, does not create the proper Active Directory associations/permissions to allow CICR replication to start and log into the customer instances in order to perform configuration changes.

For NAM to CICM replication:

Via Active Directory Users and Computers, the Service Group from the NAM instance (FAC1_CUST1_Service) must be added as a member of the service group at the ROOT OU level within the domain where the customer instance(s) reside. This must be done via Active Directory Users and Computers, and not via ICM Domain Manager tool.

Details are found in the tech tip:

CRPL (CICR Replication) Fails after Upgrade from Cisco Unified ICM Hosted Edition to ICM 7.0 with Access Error Code 9986

Document ID: 70536

http://www.cisco.com/en/US/products/sw/custcosw/ps5053/products_tech_note09186a00806c6609.shtml

For NAM to NAM replication:

Using the Active Directory Users and Computers tool, manually add the slave NAM logger Domain user into the local Administrator group on the Provisioning NAM logger machine.

Outbound Option: Call Marked Closed when Transfer to IVR/Agent on AMD

Once transferring to an agent or to an IVR is configured, there is no way to set the AMD records as Retry. You must use a customized query to identify such calls and create a new campaign.

WebView Real-Time Data and Peripheral Gateway (PG) Failover

If there is a failover in the Peripheral Gateway (PG), the WebView real-time data is set to zero. The real-time data is built up again after the failover, if the PG supports reconstructing the real-time data from the switch.

Agent Reports Roll Up Agents Based on Last Name and First Name

If the first name and the last name of two agents are same, the reporting data for both agents will be grouped under one single name and thus cause confusion. Therefore, when you add new agents using the Agent Explorer tool in the ICM Configuration Manager, ensure that the agent names are unique.

Customized Windows Operating Systems Are Not Supported

ICM/IPCC is qualified to work only on a standard, Retail (or OEM) packaged installation of Windows Server 2003 (Standard or Enterprise), with or without Cisco Security hardening. Cisco provides its own security hardening policy to secure the standard Windows image for ICM/IPCC.

Cisco does not support ICM/IPCC on a customized Windows image (for example, a corporate image) or when custom security hardening has been applied.

Customized images of the Windows operating system or customer security hardening can cause the ICM/IPCC application to fail.

Average Speed of Answer (ASA) Report Calculation

The Average Speed of Answer (ASA) value displayed in some reports, such as Enterprise Skill Group reports, might show an inflated value.

ASA is defined as a calculation of Skill_Group_Half_Hour.**AnswerWaitTimeToHalf** / Skill_Group_Half_Hour.CallsAnsweredToHalf.

AnswerWaitTime is further defined as a value made up of four individual counts: DelayTime, RingTime, LocalQTime and NetQTime. These four values are fields in the Termination Call Detail table.

A registry value has been added which is *disabled* by default. When this value is *disabled*, the calculation of AnswerWaitTime changes such that the four counts cited above are NOT used for AnswerWaitTime. In their place, a value named SkillGroupDelayQTime is used to populate the AnswerWaitTime that subsequently is used ASA calculation.

The value tracked by SkillGroupDelayQTime calculates from the beginning of the call treatment and is not reset for each delivered event, resulting in inflated values.

SkillGroupDelayQTime is not a database value in the Termination Call Detail table but is defined by the Call Router and can be found in the RTR log within the *DeviceTargetPreCallInd_V7* and *ICCallPreRouteInd_V6* events. The function of this value is controlled in the registry.

The default value of 0 for the registry value 'DeliveredEventsResetASACalculation' causes SkillGroupDelayQTime to be used for the AnswerWaitTime. When this registry value is enabled (set to 1), AnswerWaitTime is reset after the delivered event is received and will only include the time after being reset.

System IPCC Enterprise Deployment Installation and CTI OS Server

- The System IPCC Enterprise deployment installer automatically installs CTI OS Server on the Agent Controllers. You should not run the CTI OS Server installer manually. Doing so may cause your installation to fail.
- System IPCC Enterprise deployment does not support CTI OS QoS (QoS from CTI OS Client to CTI OS Server) as this turns off skill group and agent statistics.
- System IPCC Enterprise deployment does not support CTI OS Server – CTI OS Client security.

System IPCC Enterprise Deployment, ICM Setup, and WebView

System IPCC Enterprise deployment has its own streamlined installation; therefore, comments made within these Release Notes, regarding ICM Setup, generally have no bearing on System IPCC Enterprise deployment.

Similarly, System IPCC Enterprise deployment automatically installs WebView and its appropriate third-party tools. Therefore, statements made within these Release Notes regarding options related to the installation of WebView are not applicable for System IPCC Enterprise deployment. For more information, refer to the *WebView Installation and Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

System IPCC Enterprise Deployment and Date Formats

If System IPCC is installed on French, German, or Spanish platforms, date format in the EAServer .ini file (pbodb100.ini) must be changed for WebView to be able to retrieve data correctly. Follow the procedure below to change the date format fields:

Step 1 Navigate to <drive>:\Program Files\Sybase\EAServer\PowerBuilder.

Step 2 Open the pbodb100.ini file.

Step 3 In the [MSSQLSERVER_DATETIME] section, replace the following two lines

```
PBDateFmt = \ yyyy-mm-dd\
PBDateTimeFmt = \ yyyy-mm-dd hh:mm:ss.fff\
```

with

```
PBDateFmt = \ yyyy-dd-mm\
PBDateTimeFmt = \ yyyy-dd-mm hh:mm:ss.fff\
```

Step 4 Save the change.

System IPCC Enterprise Deployment Not Supported with IPCC Hosted Edition

IPCC Hosted Edition does not support System IPCC Enterprise deployment.

System IPCC Does Not Support CVP

Customer Voice Portal is not supported by System IPCC Enterprise deployment or the IPCC System PG.

System IPCC Is Only Supported on an MCS Server

System IPCC Enterprise deployment is supported only on MCS hardware.

System IPCC Service Release Installation

When installing System IPCC, the latest Service Release must be applied after installation has completed and before the Deployment Wizard has been run.

Multi-Channel Options and New Security Features

Multi-channel applications do not currently support the newly implemented 'Automated Server Hardening', 'Windows Firewall Config', or 'SSL'. Media Blender is the only exception, when it is running co-located with a PG.

Multi-Tenant CTI OS

Multi-tenant CTI OS is a new IPCC Hosted Edition feature that is only supported with Cisco Customer Voice Portal (CVP) providing network queuing on the NAM. Refer to the *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)* for sizing information.

Clustering over the WAN is supported in this environment.

Dynamic Agent Re-Skilling Restrictions for IPCC Hosted Edition

The web-based interface for re-skilling agents is installed on a Distributor AW and can only communicate with the Distributor's primary instance. If users want to do web-based re-skilling on multiple instances, they must install a separate Distributor for each instance.

ICM Hosted Edition Does Not Support IPCC Gateway

Currently ICM Hosted Edition does not support IPCC Gateway.

IPCC Express/PG Co-Residency

When a PG is installed on an IPCC Express server, its SNMP data is not available. The PG is installed with the IPCC Enterprise SNMP infrastructure, but IPCC Express (CRS) uses the Windows SNMP infrastructure. Since the two SNMP infrastructures are not compatible, only the CRS or the PG SNMP data can be made available, not both. As a result, only the CRS SNMP data is available on a server hosting both CRS and a PG.

Note that, in this configuration only, the PG may be installed on the Cisco IPT operating system version supported by IPCC Express.

ICM Partitioning

Because of such defects as CSCsb23772 and CSCsb32856, customers using, or wishing to use, ICM Partitioning are encouraged to wait until an upcoming Service Release resolves these defects before upgrading to Release 7.0(0), or newly installing Release 7.0(0) with the Partitioning option enabled.

Avaya DEFINITY Dialer Not Supported on Windows Server 2003

The Outbound Option on Avaya DEFINITY is not currently supported on Windows Server 2003 with Dialogic System Release 6.0 drivers. The Dialer should be running on a separate Windows 2000 server and cannot be collocated with the PG.

RMS Not Supporting Automated Security Hardening on Windows Server 2003

RMS is not supporting automated security hardening on Windows Server 2003.

RMS Not Supporting Windows Server 2003 SP1 Firewall

RMS is not supporting the Windows Server 2003 SP1 firewall.

Restriction of 20 Skill Groups per Agent in Release 7.0(x), 7.1(x)

With ICM / IPCC Enterprise and Hosted releases 7.0(x) and 7.1(x), the maximum supported value for Skill Groups per Agent is 20. Cisco is aware of potential issues that might occur when Agents are configured to have more than 20 Skill Groups. They include but are not limited to

- Agents cannot login in under certain conditions
- CTI Desktop buttons are grayed out
- Unable to control call state from CTI desktop
- Incorrect Skill Group data is provided

The previously published limit of 50 for Skill Groups per Agent in the 7.0 SRND is not correct.

ICM / IPCC Enterprise and Hosted release 7.2(1) will support a maximum of 50 Skill Groups per Agent. Customers who are planning to deploy release 7.0(x) or 7.1(x) and need more than 20 Skill Groups per Agent should delay their deployment until release 7.2(1) is available.

Customers who have already deployed on ICM / IPCC release 7.0(x) and 7.1(x) and are already using more than 20 Skill Groups per Agent should contact Cisco TAC to evaluate the potential issues. TAC will evaluate these issues in order to come up with an interim solution until release 7.2(1) is generally available.

Dialed Number Help for the "Permit Application Routing" Attribute in System IPCC

The online help provided for the "Permit Application Routing" attribute in System IPCC may be incorrect on your system.

The correct definition is:
(Checkbox) Allows Application Routing. Indicates if remote routing is permitted on this dialed number/script selector.

Accessing Schema Help from ICM Master Help On a Limited AW (CSCsv77964)

An error occurs when you attempt to access the Schema help from ICM Master Help. This occurs because Schema help is not installed on a Limited AW. To prevent this error, copy the *schema.chm* file from the icm\bin directory of any other type of AW and paste it into the icm\bin directory of the Limited AW.

Resolved Caveats in This Release

Resolved caveats are no longer listed in these Release Notes. Instead, you can find the latest resolved caveat information through Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

Tips You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log onto http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Bug Toolkit

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Procedure

Tips To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Step 1 Log on with your Cisco.com user ID and password.

Step 2 Click the **Launch Bug Toolkit** hyperlink.

Step 3 If you are looking for information about a specific caveat, enter the ID number in the "Enter known bug ID:" field.

To view all caveats for Cisco ICM/IPCC Enterprise and Hosted Editions, go to the "Search for bugs in other Cisco software and hardware products" section, and enter **Cisco Unified Intelligent Contact Management Enterprise** in the Product Name field. Alternatively, you can scroll through the product name list and click **Cisco Unified Intelligent Contact Management Enterprise**.

Step 4 Click **Next**. The Cisco Unified Intelligent Contact Management Enterprise search window displays.

Step 5 Choose the filters to query for caveats. You can choose any or all of the available options:

a. Select the Cisco Unified Intelligent Contact Management Enterprise Version:

- Choose the major version for the major releases.

  A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.

- Choose the revision for more specific information.

  A revision release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.

b. Choose the Features or Components to query; make your selection from the "Available" list and click **Add** to place your selection in the "Limit search to" list.

To query for all caveats for a specified release, choose "All Features" in the left window pane.

Note The default value specifies "All Features" and includes all of the items in the left window pane.

c. Enter keywords to search for a caveat title and description, if desired.

Note To make queries less specific, use the All wildcard for the major version/revision, features/components, and keyword options.

d. Choose the Set Advanced Options, including the following items:

- Bug Severity level—The default specifies 1-3.
- Bug Status Group—Check the Fixed check box for resolved caveats.
- Release Note Enclosure—The default specifies Valid Release Note Enclosure.

e. Click **Next**.

Step 6 Bug Toolkit returns the list of caveats on the basis of your query. You can modify your results by submitting another query and using different criteria.

Open Caveats in This Release

This section contains a list of defects that are currently pending in ICM/IPCC Enterprise and Hosted Editions Release 7.0(0). Defects are listed by component and then by identifier.

Tips If you have an account with Cisco.com, you can use the Bug Toolkit to find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than is reflected in this document. To access the Bug Toolkit, log onto http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Table 1 Open Caveats for Cisco IPCC/ICM Enterprise & Hosted Editions Release 7.0(0)

Identifier	Component	Headline
CSCsb22298	aw	UpccInit fails when domain\username > 30 chars
CSCsd97211	aw	Cisco ICM Service set to automatically start intermittently do not start.

Table 1 Open Caveats for Cisco IPCC/ICM Enterprise & Hosted Editions Release 7.0(0)

Identifier	Component	Headline
CSCsb02185	aw-bulk.config	Scheduled target label removed when cust name is changed
CSCsc21457	aw.conapi	Can't make config changes because CmsNode exits unexpectedly
CSCsb06385	aw.config	ICM Users are unable to delete items from Peripheral Monitor Table.
CSCsb13265	aw.config	With AutoConfig on Service Member operations should be allowed
CSCsb23772	aw.config	No user is able to create a Network VRU Script on a partitioned system
CSCsb32856	aw.config	Users can't view or manage objects in a partitioned system
CSCsg05515	aw.config	User list tool crashes while updating more than 25 users
CSCsa52733	aw.config.ba	Auto Answer should be disabled in SG tab of Campaign Config
CSCsb16721	aw.config.ba	Auto Answer field should be disabled for IPCC/Generic PG
CSCsb24392	aw.config.ba	Cannot save Agent Campaign with IP AMD and Xfer to IVR option
CSCsa53022	aw.config.list	User List does not give error when password does not meet domain policy
CSCsb07656	aw.config.list	Person List not properly displaying Japanese characters in the list
CSCsb10271	aw.config.list	Dialed Number List slow when over 175,000 DN and 300,000 Labels exist
CSCse82882	aw.config.list	Users removed from security groups following edit via User List Tool
CSCsb22880	aw.trans.route.wiz	Unable to create translation route using TR wizard in partition system.
CSCsb20552	ctios.setup	SIPCC Install/CTIOS Server Install: Missing EMSTraceServer key
CSCsa90212	db.HDS.replication	HDS gets duplicate rows; may use up memory and cause process crash
CSCsa21674	db.icmdba	Icmdba tools error messages missing specifics
CSCsa36088	db.logger	Long time to Update Agents.
CSCse61084	db.upgrade.edmt	Migrate Users called unnecessarily and could lose user information
CSCsb30829	documentation	Service Level LAA only looks at Agents logged into Priority 1 skill set
CSCsd42625	documentation	Must change Dialer phones in CCM after ICM 5.0 pre-SR4 to ICM 7.0 upgrd
CSCsf24951	documentation	User in the configuration group is unable to start configuration tools
CSCsb26062	ipccinstall	scheduled jobs to prune/purge hst/ems log files aren't added at install
CSCse81495	ipccinstall	Can't read from db if TCP/IP not enabled in SQL Server Network Utility
CSCsa99530	ipccwebconfig	System information pages hang if all machines are not reachable via net
CSCsb14823	ipccwebconfig	SIPCC needs to allow setting Low and High network priorities.
CSCsb27612	ipccwebconfig-ui	Need to remove Outbound Access options from Agent Desk Settings
CSCsb27515	pg.definity	PIM sending invalid trunk information to OPC
CSCsb29349	pg.definity	Outbound call gets disconnected.
CSCsb27767	pg.dms100	DMS PIM Fails to Go Active on Restart Due to Eicon Card Init Timing
CSCsa89635	pg.mrpim	Chat requests are stuck in Q: MR PIM call var length exceeded
CSCsb03835	pg.opc	Missing half hour aggregate records when PG CPU pegs for long time
CSCsb14124	pg.symp	Real time data not getting updated
CSCsb29263	pg.symp	Problem with consultation transfert from IDN call to IDN.
CSCsb01893	pg.symp.noseipim	Customer Abandons,Consult Call is cleared when a new call initiated

Table 1 Open Caveats for Cisco IPCC/ICM Enterprise & Hosted Editions Release 7.0(0)

Identifier	Component	Headline
CSCsb14877	pg.vru	OriginatorType value of 70 appeared in RCD, which should be 0 - 4.
CSCsb22885	reporting.monitoricm	Unable to connect to customer ICM (CICM) server using CICM Monitor tool.
CSCsa49786	reporting.webview	Hold time summary data not populating in persvc26
CSCsa82572	reporting.webview	username and logout does not appear in webview footer after SR uninstall
CSCsb02382	reporting.webview	Report Item List Box does not return all items with large configurations
CSCsb04030	reporting.webview	Corruption in the description of saved reports in JPN,CHS,KOR
CSCsb06606	reporting.webview	Scheduled jobs don't complete when SSL is used
CSCsb06693	reporting.webview	Listing scheduled reports is sensitive to the case of instance in URL
CSCsb19659	reporting.webview	Can't export graphical reports to HTML Table format
CSCsb04968	router	Router.exe spikes to 100% processor utilization at midnight
CSCsb07382	router	NAM Router Script ??? (ID 0) failed to produce route for dialed number
CSCsb08093	scripteditor	Script Editor does not allow AgentToAgent node for Simplified peripheral
CSCsa64411	setup	updateaw restarts - default distributor user denied access to central DB
CSCsa73173	setup	NAM Logger user doesn't have read access to Provisioning NAM Database
CSCsb36857	setup	The url to Dynamic Reskilling is missing when installed with icm setup
CSCsb54339	setup	Dynamic reskilling fails after using ICM setup to edit AW
CSCse55800	setup	Cannot replicate configuration changes from NAM to CICM
CSCsf00181	setup	Central Controller private network may be negatively impacted.
CSCsd84862	setup.aw	Local Setup fails on Limited AW system
CSCse55500	setup.webview.ICM	Jaguar service will not start after another webview instance is deleted.
CSCsb44273	setup.3rdparty	New Atlanta Servlet cannot be installed on some W2003 server (SPA,FRE,..
CSCsb35269	voicecsa	CSA sometimes wont let ICMSetup start.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Instructions for ordering documentation using the Ordering tool are at this URL:

  http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Product Alerts and Field Notices

Cisco products may be modified or key processes may be determined important. These are announced through use of the Cisco Product Alert and Cisco Field Notice mechanisms. You can register to receive Product Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest. Log into www.cisco.com; then access the tool at http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html