Release Notes for *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.2(1)*

January 8, 2009

Updated Information in this Document

This document updates the November 24, 2008 version with the following changes:

Section and Page	Notes	Date Added
Cycling PG After Changing Agent ID, page 32	Provides information about process to complete when the Agent ID (Peripheral ID) changes.	8Jan2009
Accessing Schema Help from ICM Master Help On a Limited AW (CSCsv77964), page 21	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
Outbound Option: Registry Keys, page 19	Provides information on the registry keys CancelDialingCalls, ThrottlingUpValue, ThrottlingDownValue, MaxPortCapacityReachedCount	24Sep2007
Campaign Manager, page 17	Discusses backward compatibility for Release 7.2(1) Campaign Manager.	10Sep2007

Contents

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

© 2007 Cisco Systems, Inc. All rights reserved.

Introduction

ICM/IPCC software Release 7.2(1) supports ICM and IPCC Hosted & Enterprise Editions. This document discusses new features, changes, and caveats for Release 7.2(1) of ICM/IPCC Enterprise and Hosted software.

This document is a supplement to both the *Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(1)* and the *Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0)*, both of which are available at:
http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_release_notes_list.html

The 7.2(1) Release Notes should be used in conjunction with both of the above Release Notes.

About Release 7.2(1)

Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.2(1) is a minor release. New as of Release 7.1(1), a minor release is an incremental set of defect fixes and a limited set of new functionality delivered in an automated installer.

As of ICM Release 7.1(x), Service Releases are being renamed to Maintenance Releases.

A minor release is incremental, cumulative to the base release of the Major release. A minor release can be returned to its pre-installation state. All ongoing maintenance release content present at the point of the minor release ship date is contained within the minor release. The only exception is where a minor release development/testing schedule overlaps with that of a maintenance release. Engineering specials released prior to the code freeze date are also part of the minor release content.

Minor Release 7.2(1) can be installed over ICM/IPCC 7.0(0) [including any Service Releases], or ICM/IPCC 7.1(x) [prior to ICM/IPCC 7.1(5)]. The Release 7.2(1) Installer performs a check that prevents it from installing on systems running ICM/IPCC 7.1(5).

The minor release is available on CD and as downloadable installers from cisco.com.

For additional information on the Cisco software support methodology, refer to the *ICM/IPCC Enterprise Maintenance Support Strategy*, available at:
http://www.cisco.com/kobayashi/sw-center/telephony/icm/icm-planner.shtml (requires login).

ICM/IPCC 7.0(0) must be installed prior to installing Release 7.2(1). For an explanation of the specifications for ICM/IPCC Enterprise & Hosted Edition Release 7.0(0), refer to the C*isco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)*, which is accessible from:
http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

Release Notes for *Cisco CTI Object Server*, *Cisco Agent Desktop*, *Cisco E-Mail Manager Option*, *Cisco Support Tools,* and *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.

For a detailed list of language localizations implemented for different portions of this release, refer to the Cisco Unified ICM/Contact Center Product and System Localization Matrix available at: http://www.cisco.com/application/vnd.ms-excel/en/us/guest/products/ps1846/c1225/ccmigration_09186a008068770f.xls

Note The most up-to-date version of these release notes is available on the Web at: http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_release_notes_list.html

A Note about Product Naming

Cisco IPCC Enterprise Edition is being renamed to Cisco Unified Contact Center Enterprise (abbreviated as Unified CCE).

Cisco IPCC Hosted Edition is being renamed Cisco Unified Contact Center Hosted (abbreviated as Unified CCH).

Cisco Intelligent Contact Management (ICM) Enterprise Edition is being renamed to Cisco Unified Intelligent Contact Management Enterprise (Unified ICME).

Cisco Intelligent Contact Management (ICM) Hosted Edition is being renamed to Cisco Unified Intelligent Contact Management Hosted (Unified ICMH).

Cisco CallManager/Cisco Unified CallManager is being renamed to Cisco Unified Communications Manager.

These new names are introduced in this release for Agent and Supervisor product opening-screens and in documentation that has been revised for Release 7.2(1), but they do not yet appear throughout the user interface or documentation. These release notes use the previous naming convention.

System Requirements

For hardware and third-party software specifications for Release 7.2(1), refer to the *Hardware and System Software Specification (Bill of Materials): Cisco ICM/IPCC Enterprise & Hosted Editions*, which is accessible from http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

Release 7.2(1) updates are also available for CTI OS, Cisco Agent Desktop, and Unified Contact Center Management Portal. Cisco E-Mail Manager and Cisco Web Collaboration Option remain at Release 5.0.

See the *Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.2(1)* for information on agent desktop and PG software versions supported during 7.2(1) migration, as well as other important upgrade considerations.

Installation of Release 7.2(1) has a prerequisite of a Release 7.0(0) base installation, as described in the above document.

Related Documentation

Documentation for Cisco ICM/IPCC Enterprise and Hosted Editions, as well as most related documentation, is accessible from http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

- Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) - http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_release_notes_list.html
- Related documentation includes the documentation sets for Cisco CTI Object Server (CTI OS), Cisco Agent Desktop (CAD), Cisco Agent Desktop - Browser Edition (CAD-BE), Cisco Unified Contact Center Management Portal, Cisco E-Mail Manager Option, Cisco Web Collaboration Option (including Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender), Cisco Unified Customer Voice Portal (CVP), Cisco IP IVR, Cisco Support Tools, and Cisco Remote Monitoring Suite (RMS).
- Also related is the documentation for Cisco Unified 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

Note New features available in the accompanying release of CTI OS are discussed in the *CTI OS Release Notes for Release 7.2(1)*).

New features available in the accompanying release of Cisco Agent Desktop (CAD) are discussed in the *Cisco Agent Desktop Release Notes for Release 7.2(1)*).

New features available in the accompanying release of Cisco Unified Contact Center Management Portal are discussed in the *Release Notes for Cisco Unified Contact Center Management Portal Release 7.2(1)*.

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

Intelligent Contact Management (ICM) and IP Contact Center (IPCC) software Release 7.2(1) is a minor release that contains fixes and a limited set of new functionality. All previous service releases to Release 7.0(0), as well as 7.1(1) and all its maintenance releases [prior to 7.1(5)], are included in Release 7.2(1). That is, Release 7.2(1) is incremental and cumulative, and can be rolled back.

Release 7.2(1) introduces the following new features:

- ICM Database Schema Changes, Release 7.1(1) to Release 7.2(1), page 8
- Technical Changes and Notes, page 7, provides information on new features that are more technical in nature.

CallManager-Based Silent Monitoring

For Release 7.2(1), a new CallManager 6.0-based Silent Monitoring implementation is being introduced.

This implementation is mutually exclusive with the legacy CTI OS-based Silent Monitoring.

The CallManager-based Silent Monitoring session consists of an Agent using an IP hard phone being monitored by a Supervisor using either the CAD or CTI OS Toolkit desktop. The Supervisor listens to the monitored session on their IP hard phone.

Current advantages and disadvantages associated with using the CallManager-based silent monitoring are:

Advantages

- No Network Interface Card restrictions.
- Any 7.x version of any desktop (C++, Java, .Net, Siebel) can be silent monitored provided the agent is not a mobile agent.
- Silent monitor is implemented via a call therefore the silent monitor call is carried on the voice LAN. With CTI OS silent monitor, the silent monitor stream is carried on the data LAN.
- Silent monitor calls are reported as agent-to-agent calls for supervisors. With CTI OS silent monitor, supervisor's time spent silent monitoring is not tracked.

Disadvantages

- Agents using phones other than 79x1 phones (7941, 7961, or 7971) cannot be silent monitored.
- Agents using IP Communicator cannot be silent monitored.
- Supervisors using 7.1(x) or earlier desktops cannot initiate CallManager silent monitor.
- CallManager silent monitor is not supported with CallManager 5.x and earlier.
- Mobile agents cannot be silent monitored.

Note For System IPCC, configuration of the Silent Monitor mode is in the Web Administration tool.

Avaya Agent Routing Service (ARS)

The Avaya ARS Gateway provides the interface between the ARS PIM and the Avaya PBX. The ARS PG is connected to the PBX utilizing the Avaya ASAI interface.

The ARS PG translates call control, call events, device monitoring, and call routing messages between the ARS PIM and the PBX. It also maintains the heartbeat and connection between PIM and PBX.

For additional information see the *ARI Deployment Guide for Cisco Unified Intelligent Contact Manager Enterprise* and the *System Manager Guide Supplement for Avaya ARS PG*.

Cisco Security Agent (CSA) 5.0

A newer standalone version of CSA for Cisco ICM/IPCC Enterprise and Hosted Editions, based on CSA engine version 5.0, is available for ICM/IPCC Enterprise & Hosted Release 7.2(1). For more details refer to the *Cisco Security Agent Installation/Deployment Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.2(1)*.

CSA 4.5.1, which was supported on prior releases of ICM/IPCC Enterprise, is not supported in Release 7.2(1). Hence, you must uninstall CSA 4.5.1 prior to upgrading to Release 7.2(1). 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. The Release 7.2(1) installer automates 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.

Russian and Traditional Chinese Localization

In addition to retaining support for localizations in earlier releases, Release 7.2(1) provides localization for Russian and Traditional Chinese. This involves support for the following SQL collations: Cyrillic_General_BIN and Chinese_Taiwan_Stroke_BIN. See the *Installation Guide Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.2(1)* for a more detailed discussion of localization.

Support Tools 2.1 Node Agent Bundling

ICM/IPCC Release 7.1(1) introduced bundling and installation by default (but not enabling) of the Support Tools Node Agent. Release 7.2(1) furthers manageability of the solution by default enabling of the Support Tools Node Agent (under certain security requirements). A configuration dialog is invoked during patch installation querying for a pre-shared key. The Release 7.2(1) patch installer invokes the silent installer for Support Tools Node Agent 2.1, passing it this pre-shared key and instructing the Node Agent to enable itself. That key will be used subsequently by the Support Tools 2.1 Node Agent to authenticate any Support Tools Server requests.

The patch installer also invokes the IPSec scripts that enable IPSec filtering for authentication (not encryption). Enabling of Support Tools Node Agents out-of-the-box will ease the trace setting and log collection process for ICM/IPCC Enterprise & Hosted deployments.

The authentication which is done between Support Tools Server and Node Agent, as mentioned above, is through an IPSec Security Policy. This IPSec Security Policy is the one which is installed by the Patch Installer.

Note that re-installation/upgrade of Support Tools disables service. For the latest information on this problem, access CSCse71886 through Bug Toolkit.

Drill-Down Enhancement for Reporting

Note The drill-down feature exists only for some non-graph reports.

If users want to use the drill-down feature, they would first generate a report and then go to the Drill Down page and choose the sub-report they want to run.

Further, a default drill-down sub-report that supports this feature has been added to the templates such that a customer can launch a detailed sub-report from within the current report page without going to the Drill Down page.

Users can also change their choice of drill-down report by going to the Drill Down page and selecting a different detailed sub-report.

Configuration Scalability Limit Enhancements

The number of Skill Groups that an Agent belongs to will be validated, and an error returned if that number is greater than the maximum allowed. The default value is 50. However, the limiting value can be changed by an Administrator if there is a compelling reason to do so. See Modifying the Skill Groups per Agent Limit, page 36.

Also see Failure Occurs when Agent with 50 Skills Logs In on Child IPCC System, page 20.

Technical Changes and Notes

The following changes in Release 7.2(1) are generally of a more technical nature than those above.

Event Message Enhancements

A standard event message format for the syslog protocol has been provided that is consistent with the CiscoLog format. This is in line with ensuring a consistent solution-level event format, which will ultimately ease and speed troubleshooting efforts and greatly aid event correlation logic/rules.

Expanded Call Variables (ECC) List Tool Warning on CTI Server Byte Limit

The Expanded Call Variables (ECC) List Tool tool warns of a 2500 byte CTI Server limit if that the limit is exceeded. This limit is calculated as follows:

For Scalars:

The total number of bytes for the name + the maximum length of data + 4

For Array entries:

The size of the array * (The total number of bytes for the name + the maximum data length of data + 5)

Note that if an array is 10 elements, the name is repeated, and counted, 10 times. Also note that the string 'user.' prefixes all of the names, so it counts as 5 on every scalar or array element.

The sum of the values computed by the above formulas for all configured variables must be less than 2500 bytes.

JDK and JRE are updated to JDK1.4.2_13 and JRE 1.4.2_13

The updating of JDK and JRE occurs on

- Distributor AW systems with CMS and/or the Agent Re-skilling Web Tool enabled
- IPCC System Peripheral Gateway (PG) systems
- WebView systems
- CallManager Peripheral Gateway (PG) systems
- System IPCC systems with the role of Administration and WebView Reporting

Security Enhancements

Various security enhancements have been made regarding Active Directory, Security Best Practices, and Port Utilization. These are documented in the appropriate manuals.

ICM Database Schema Changes, Release 7.1(1) to Release 7.2(1)

This section indicates the changes made to the ICM/IPCC Database Schema between Release 7.1(1) and Release 7.2(1). Refer to the *Database Schema Handbook for Cisco ICM/IPCC Enterprise & Hosted Editions* for descriptions of the new tables and columns.

The changes to the database schema are made atop of Release 7.0(0) or Release 7.1(1), as part of the Release 7.2(1) installer. The EDMT utility is not used in this upgrade process.

Installing 7.2(1) on 7.0(0) will make the changes contained in both 7.1(1) and 7.2(1). However, only the differences between 7.2(1) and 7.1(1) are discussed here. The differences between 7.0(0) and 7.1(1) are discussed in the *Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(1)*.

Database changes can be rolled back.

Tables Added

Configuration Limit

Dialer_Detail (for future use)

Changes to Existing Tables

Agent_Real_Time

Column(s) Added
FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5

Agent_Skill_Group_Real_Time

Column(s) Added
FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5

Blended_Agent_Optionsl

Column(s) Added
FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5
FutureUseVarChar1
FutureUseVarChar2
FutureUseVarChar3

Call_Type

Column Changed
ServiceLevelThreshold from DBSMALLINT to DBINT

Campaign

Column(s) Added

FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5
FutureUseVarChar1
FutureUseVarChar2
FutureUseVarChar3
FutureUseFloat1
FutureUseFloat2
FutureUseFloat3

Campaign_Skill_Group

Column(s) Added

FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5
FutureUseVarChar1
FutureUseVarChar2
FutureUseVarChar3

Campaign_Target_Sequence

Column(s) Added

FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5
FutureUseVarChar1
FutureUseVarChar2
FutureUseVarChar3

Dialer

Column(s) Added

FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5
FutureUseVarChar1
FutureUseVarChar2
FutureUseVarChar3

Dialer_Half_Hour

Column(s) Added

FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5

Dialer_Port_Map

Column(s) Added

FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5
FutureUseVarChar1
FutureUseVarChar2
FutureUseVarChar3

Dialer_Port_Real_Timep

Column(s) Added

FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5
FutureUseVarChar1
FutureUseVarChar2
FutureUseVarChar3

Dialer_Real_Time

Column(s) Added
FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5
FutureUseVarChar1
FutureUseVarChar2
FutureUseVarChar3

ICR_Globals

Column Changed
CallTypeServiceLevelThreshold from DBSMALLINT to DBINT

Import_Rule

Column(s) Added
FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5
FutureUseVarChar1
FutureUseVarChar2
FutureUseVarChar3

Import_Rule_Clause

Column(s) Added
FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5
FutureUseVarChar1
FutureUseVarChar2
FutureUseVarChar3

Import_Rule_History

Column(s) Added
FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5

Import_Rule_Real_Time

Column(s) Added
FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5

Media_Routing_Domain

Column Changed
ServiceLevelThreshold from DBSMALLINT to DBINT

Query_Rule

Column(s) Added
FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5
FutureUseVarChar1
FutureUseVarChar2
FutureUseVarChar3

Query_Rule_Clause

Column(s) Added
FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5
FutureUseVarChar1
FutureUseVarChar2
FutureUseVarChar3

Service

Column Changed
ServiceLevelThreshold from DBSMALLINT to DBINT

Service_Level_Threshold

Column Changed
ServiceLevelThreshold from DBSMALLINT to DBINT

Skill_Group

Column Changed
ServiceLevelThreshold from DBSMALLINT to DBINT

Skill_Group_Real_Time

Column(s) Added
FutureUseInt1
FutureUseInt2
FutureUseInt3
FutureUseInt4
FutureUseInt5

Important Notes

The following sections contain restrictions that apply to Release 7.2(1).

Restrictions, Limitations, Scalability

In general, information on restrictions, limitations and scalability are provided in the following documents:

- The *Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0)* and *Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(1)* available at: http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_release_notes_list.html
- The *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)*, updated for Release 7.2(1), available from http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html
- The *Software Compatibility Guide for Cisco IPCC Enterprise Edition*, available from: http://cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html
- The *Cisco Unified Mobile Agent Guide for Unified CCE* provides information on limitations in the Mobile Agent feature.
- The *IPCC Solution Reference Network Design (SRND) for Cisco IPCC Enterprise Edition*.

Release 7.2(1) is a cumulative update and may rectify restrictions as documented in the ICM Release 7.0(0) Release Notes and ICM Release 7.1(1) Release Notes.

Installation

See the *Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.2(1)* for information on how to plan for and deploy Release 7.2(1), including information on agent desktop and PG software versions supported during 7.2(1) migration.

Note The Installation Guide instructs you to stop CSA during the installation. If the confirmation dialog is not displayed when attempting to stop the CSA service on a machine that has had users logged into it via a session of Remote Desktop Connection, the CSA service can not be stopped. The Installer appears to be hung while displaying the "Stopping CSA" dialog. Use the Task Manager to disconnect and logoff any users that are currently, or have previously been, connected to the system. Before attempting to stop CSA again, either allow the initial request to stop CSA to timeout (60 minutes), or reboot the system.

Campaign Manager

The Release 7.2(1) Campaign Manager is only backward compatible with Release 7.0(0) SR04 ES56 and up, or Release 7.1(3) - Release 7.1(5) Dialers.

System IPCC Upgrade

For System IPCC, any servers with the following roles must use the same release of software (for example, Release 7.2(1)):

- Central Controller
- Administration & WebView Reporting
- Outbound Controller

For example, if you upgrade your Central Controller servers to Release 7.2(1), then you must upgrade your Administration & WebView Reporting servers and Outbound Controller servers to Release 7.2(1) as well. We also strongly encourage customers to keep their machines with "Agent/IVR Controller" roles (these servers have the IPCC System PG, CTIOS Server and CTI Server) at the same version as the Central Controller if they are on a separate server.

Also, if after installing Release 7.2(1) you decide to roll back to a previous 7.x release, you do not need to delete any System IPCC machines from the database (using the Web Administration tool under *System Management* > *Machine Management* > *Machines*) unless you intend to uninstall Release 7.0(0) as well.

See Chapter 15 of the *System IPCC Enterprise Installation and Configuration Guide* for information on the install and uninstall of System IPCC.

CallManager-Based Silent Monitoring for System IPCC Requires Configuration Change

The default setting in System IPCC is CTIOS Silent Monitor. Other possible values are CCM Silent Monitor and Disabled. CCM Silent Monitor must be selected in order to use CallManager-based Silent Monitoring.

For System IPCC, configuration of the Silent Monitor mode is in the Web Administration tool.

For additional details on setting up CallManager-Based Silent Monitor, see the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise and Hosted Edition, Release 7.2(1)*.

Outbound Option: Deployment with CallManager 5.x

Deployment of Outbound Option with CallManager 5.x requires application of an ES (5.1.2.1104-2) for the CallManager defect CSCsh22852.

Outbound Option: Dialer_TCD No Longer Supported; to be Replaced by Dialer_Detail

The Dialer_TCD feature is no longer supported.

This functionality will be replaced by Dialer_Detail records, which will not be generally available until Release 7.2(2). The Dialer_Detail table includes more information than was previously available with the Dialer_TCD feature. The Dialer_Detail table will track data on all outbound attempts, including personal callback attempts and preview calls that are skipped by an agent.

Outbound Option: Custom Triggers No Longer Supported

No manual changes to the contents of the outbound database are allowed. Using triggers in the outbound database is not allowed. Triggers for the dialing lists or personal callback list should not be added or modified.

Outbound Option: Upgrading Campaign Manager and Dialer

In general, it has been true that the Campaign Manager (which is on the Logger) and the Dialer (which is on the PG) must be at the same release. This has been handled by disabling the Dialer service on the PG, upgrading the Logger, and keeping the Dialer disabled until the PG can be upgraded to the same release as the Logger. However, this creates difficulties for systems with a large number of Dialers, because of the time involved.

With Release 7.2(1), if the Campaign Manager is at 7.2(1), the Dialer can remain temporarily at

- 7.0(0) SR4 with ES 18 or equivalent

or

- 7.1(3) or later

though the Dialer should be upgraded to 7.2(1) as quickly as possible.

Outbound Option: Registry Keys

The following registry keys exist in the Dialer registry:

CancelDialingCalls: The option to control whether the predictive algorithm cancels the customer calls in progress when there is no available agent. The default is 0x00000001 (1), which means the dialer will cancel the customer call regardless of its progress unless Abandon to IVR is configured. Setting this value to 0x00000000 (0) will cause the Dialer to only cancel any calls where the customer phone has not started ringing yet. Any value greater than one will cause the dialer to cancel calls that the dialer started dialing less than that value minus one seconds ago. For example, a value of 6 will cause the dialer to cancel calls that it placed less than five seconds ago if no agents are available. Increasing this value too much increases the chance that the customer phone will ring many times before the Dialer cancels the call.

ThrottlingUpValue: Incremental value for ports per agent in the predictive algorithm when the actual abandon rate is below the configured abandon rate. The default is 0x00000001 (1).

ThrottlingDownValue: Decremental value for ports per agent in the predictive algorithm when the actual abandon rate is above the configured abandon rate. The default is 0x00000002 (2).

MaxPortCapacityReachedCount: Maximum number of times that the port availability will be exceeded before tracing a warning message, “Warning: Skill group [%d] has reached port capacity - MaxPortCapacityReachedCount=%d”. The default is 0x0000001e (30).

Internet Script Editor (ISE) and Write Privileges

The Release 7.2(1) security template hardens the file permissions on the system drive (C:). ISE users need write privileges on the c:\icm\<instance>\dis\ise folder. The assumption is that they will get those privileges by inheriting it from the parent folder(s). This assumption fails when the system drive is hardened and Release 7.2(1) is installed on the system drive.

Therefore, ISE setup (AW setup) should not assume that ISE will inherit write privileges on the above mentioned folder. ISE setup must grant write privileges to the Config Domain Security group for that ICM Instance (<facility>_<instance>_Config domain group) on the folder c:\icm\<instance>\dis\ise.

For the latest information on this problem, access CSCsi61878 through Bug Toolkit.

Security Hardening Blocks SSL Connections from Internet Explorer

Release 7.2(1) Security Hardening blocks SSL connections from Internet Explorer 6 to WebView, the Agent Re-skilling Web Tool and System IPCC Web Configuration and Web Re-skilling. SSL is enabled by default for WebView, the Agent Re-skilling Web Tool and System IPCC Web Configuration and Web Re-skilling. When the server is hardened using the release 7.2(1) Security Hardening Template and Internet Explorer 6 is used with default configuration to connect over HTTPS, an error is thrown.

Release 7.2(1) Security Hardening secures the IIS webserver such that the browser connecting to it must use TLS. Internet Explorer 6, by default, does not enable TLS support. To connect to a hardened WebView, Agent Re-skilling Web Tool or System IPCC Web Configuration and Web Re-skilling server over HTTPS using Internet Explorer 6, the following setting must be enabled in Internet Explorer 6:

Go to

1. Tools
2. Internet Options
3. Advanced
4. Scroll down to Security section
5. Enable TLS 1.0

For more information on this security setting, see Microsoft KB article 811833: http://support.microsoft.com/kb/811833

For the latest information on this problem, access CSCsg93131 through Bug Toolkit.

Failure Occurs when Agent with 50 Skills Logs In on Child IPCC System

In a parent-child deployment, when an agent configured with 50 user-defined skills on the child IPCC System PG logs in, the parent IPCC Enterprise Gateway PIM fails.

If 50 skills per agent is required, then make the following changes in the Windows Registry for the key "MaxSkills" under the IPCC Enterprise Gateway PG registry entries:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\< customer_instance >\PG{n}[A|B]\PG\CurrentVersion\PIMS\pim{m}\ACMIData\Config\MaxSkills

The key should be updated to a value of 51 from its default value of 50.

For the latest information on this problem, access CSCsi87801 through Bug Toolkit.

CTI Server Sends Call Variables with 40 Characters plus Null Terminator

There was a change in CTI Sever to support call variables of 41 byes (40+Null). However, this change breaks the downward compatibly of the CTI Server interface, since in older versions of the protocol, any call variable that was larger than 39 characters was truncated.

Some customers may have used the older limitation by placing the CTI critical data in the first 39 characters, but using the fortieth byte on the IVR, ICM, and HDS. When CTI clients attempt to use an older protocol (for example, Protocol 9), they will not receive events since they are only expecting to see 40 bytes maximum (39+null).

To avoid this problem, use only a maximum of 39 + null characters for call variables.

For the latest information on this problem, access CSCsi65928 through Bug Toolkit.

Russian WebView Online Help

The Contents pane in the Russian online help for WebView is garbled.

For the latest information on this problem, access CSCsi36159 through Bug Toolkit.

Mobile Agent

- Mobile Agent scalability may be contingent on specific CallManager versions, see the *IPCC Solution Reference Network Design (SRND) for Cisco IPCC Enterprise Edition* for Release 7.2(1) for details.
- Web Callback is not supported for Mobile Agent
- Blended Collaboration is not supported for Mobile Agent
- If a Mobile Agent calls RP (route point) or another Mobile Agent's instrument under the following conditions, the call will fail:
  - both Mobile Agents are using an SCCP phone as a mobile phone.
  - the remote call leg which is from RTP CTIPort to Mobile phone is via SIP ICT trunk.

  Workarounds are:
  - Enable MTP on SIP trunk (though note that CallManager has limited MTP resources).
  - If a SIP trunk is used, use SIP phones.
  - Instead of using a SIP trunk, use H.323.

Cisco Web Collaboration Option 5.0 and Cisco E-Mail Manager Option 5.0

Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender, and Cisco E-Mail Manager remain at the Release 5.0 version of their respective products. However, compatibility with these products and ICM/IPCC Release 7.2(1) has been maintained.

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.

Tip 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

Tip 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 7.2(1). Defects are listed by component and then by identifier.

Tip 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 ICM/IPCC Enterprise & Hosted Editions Release 7.2(1)

Identifier	Component	Headline
CSCsi43663	aas	AAS Console Window Shows Active Even When Connections are Down
CSCsi63522	aas	Skillgroups get updated in ICM even though no changes are made in SCCS
CSCsi73378	aas	AAS switches over to induvidual mode from bulk mode taking longer time
CSCsi52126	aw.conapi	CMS Node Crashes Accessing Database
CSCsb38949	aw.config	ICM Instance selection Fault with Bulk Edit and Insertion Tools
CSCsg05515	aw.config	User list tool exited unexpectedly while adding more than 25 users
CSCsi84097	aw.config	Userlist tool performance is unacceptably slow
CSCsi42776	aw.config.explorer	Trusted Domains do not appear in Agent Explorer list
CSCsi47093	aw.config.explorer	In Agent Explorer, can't associate an existing AD user as a supervisor
CSCsi51514	aw.config.explorer	Agent Explorer and User List long delays in retrieving Users.
CSCsj03276	aw.config.explorer	Unable to create supervisor in agent explorer in child domains
CSCsj07318	aw.config.explorer	Error message creating supervisor using Agent Explorer
CSCsb82435	aw.config.list	ICM user could not be deleted in partitioned system using User List tool
CSCsh19120	aw.config.list	Config Manager Extremely Slow Loading Dialed Number List
CSCsi05491	ba.dialer	Outbound Predictive Dialer takes too long to adjust the outbound rate

Table 1 Open Caveats for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.2(1)

Identifier	Component	Headline
CSCsi65381	ba.dialer	Dialer calls customer again (diff zone) after marked as wrong number
CSCsh75571	ba.dialer.ipcc	On failure, Dialer port should try to reregister w prim CCM periodically
CSCsj13119	ba.dialer.ipcc	Need to document that AutoAnswer On in CCM and Dialer is not supported
CSCsi65928	cg.ctiserver	CTI Sever Interface no longer Downward Compatible due to 40 byte CV chg
CSCsh18947	documentation	Caltyp22.htm Help Not Correct for Tasks Offered
CSCsd70960	ipccinstall	North American regions installed on System IPCC regardless of language.
CSCse81495	ipccinstall	Can't read from db if TCP/IP not enabled in SQL Server Network Utility
CSCsi72098	ipccwebconfig-ad	Assigning Admin permissions for WV slow to respond or times out on SIPCC
CSCsj11378	localization	Unacceptable CHS templates
CSCsj11402	localization	Unacceptable KOR templates
CSCsj11416	localization	Unacceptable DEU templates
CSCse77314	netwrkcic	CIC asserts with C0000005 ACCESS_VIOLATION on procmon LTM command
CSCsj11920	nic.incrp	7.0+ CICM (INCRPNic) with Pre 7.0 NAM will fail if Release node used
CSCsi87801	pg.acmi	ACMI PIM crashes when Agent with 50 Skills logs in, on Child IPCC System
CSCsg87590	pg.ars	(1346)ARS Agent can login with same invalid extension in the second try
CSCsi10213	pg.ars	Intercept not getting updated in skill group hist reports for ARI
CSCsh95253	pg.definity	ECS PIM asserts with DrWatson
CSCsi63543	pg.eapim.jtapigw	CTIOS client freezes and consult call drops with mult calls to same DN
CSCsi46353	pg.neax2400	NEC PIM Reason Code for Break is always 1
CSCsi07769	pg.opc	transferred out conference call fails to deliver to agent
CSCsi25230	pg.opc	Incorrect Short Call Detection from Siemens HICOM PIM
CSCsi56723	pg.opc	Agent stuck on wrapup when transferring the call
CSCsi65765	pg.opc	Peripheral reports run from Parent ICM are offset
CSCsi78305	pg.opc	OPC:Active tasks still showing non-zero value even when no calls active.
CSCsj30070	pg.opc	OPC mem usage keeps growing during Outbound Option load
CSCsi40583	reporting.webview	The Skill Group summaries for BusyOther (% and Time) are missing.
CSCsi33069	router	CICM Router Crashed
CSCsi47922	router	Calculation of DelayQAbandTime Incorrect
CSCsc70418	scripteditor	Router did not end the scripts at the specified date time
CSCsi10483	security	The Webview login is slow or times out causing the user login to fail
CSCsb41422	setup	Instance name used in >1 OU may fail to upgrade; permission not granted
CSCse55800	setup	Cannot replicate configuration changes from NAM to CICM & NAM to NAM
CSCsi11987	setup	Unable to open historical reports when AW and Webview on diff machines
CSCsi84096	setup	Scheduled jobs not removed and duplicates created rerunning setup.
CSCsi58149	setup.pg	Cannot uninstall AAS
CSCse55500	setup.webview.ICM	Jaguar service will not start after another webview instance is deleted.

Troubleshooting

Troubleshooting information is available in the product documentation. Additional troubleshooting tips appear below:

Setup Troubleshooting

Finding the Release 7.2(1) log

The Release 7.2(1) Installer's setup log is in the following folder on the system drive. (All examples assume system drive is C:). Example: C:\temp\Minor Release ICM7.2(1)

- New log files are created each time the installer is run, with unique IDs of format YYYYMMDDHHMM, is pre-pended to the file name "_Minor Release ICM7.2(1).log". Example: *20060404_112338_Minor Release ICM7.2(1).log*
- JDK/JRE installation logs are embedded within the Minor Release installer's log.
- Support Tools setup log is created or appended to existing log file. Example: *C:\temp\ICM_SupportTools_Setup.log*
- Schema Upgrade/rollback logs. Example: *C:\temp\<server name><instance name><DB name>.log*

error -9934

Symptom: On a AW Client only system, running Configuration Manager may display the error "-9934. Unable to initialize real-time feed for instance."

Reason: The real-time feed error is caused by ICM7.0FCS real-time distributor which has not been applied with 7.2(1) release.

Solution: Make sure the Release 7.2(1) is applied on the Distributor, Call Router and the Logger, then bring up the Call Router, Logger, and Distributor services.

Failure to stop Tomcat service

Symptom: During the Release 7.2(1) installation or uninstallation, installer attempts to stop the Apache Tomcat Service, if it is running. On some systems, the installer may report a failure to stop the service, and abort the installation.

Reason: When stopping service reports error, before passing error on the installer goes into a loop to test for a file lock on tomcat5.exe. It does retries at 5 sec intervals for 3 minutes. If lock does not release in 3 minutes, then error gets passed on.

Solution: Go to the system's "Services" console, and manually stop the Tomcat service. Restart the installer.

Error in log: Failure stopping Jaguar Watchdog

Symptom: During the minor release installation or removal, setup automatically stops the Jaguar Watchdog Service. Occasionally, an error message is written to the setup log that stopping the service failed. The installer continues to run.

Solution: Look in the Services window to find out if the service is running or not.

File lock error message

Symptom: If an ICM application is running when the installer starts (Script Editor, for example) the operating system applies a lock to files loaded into memory, blocking the update of those files. The installer will abort, explain that an ICM application is currently running, and list the locked files.

Reason: Launching install or uninstall without stopping ICM non-service programs. (Note that running ICM services are automatically stopped and will not lead to this message.)

Solution: Stop all ICM programs before installing or uninstalling the minor release. If you can't find a running application, try looking for the locked file as a process in Task Manager, and shut it down there.

Database

Incompatible Schema Versions

Symptoms:

- Logger displays "Major Version Mismatch!"
- You can not run ICM 7.0 with a database schema from ICM 7.2.

Reason: This can happen after a temporary uninstall (without schema downgrade), and then running ICM services

Solution: Reinstall ICM 7.2(1)

Note If you wish to go back to running ICM 7.0(0), you must perform a **permanent** uninstall (with schema rollback).

Incompatible Schema Versions (other)

Symptoms: Logger displays "The sideX Logger cannot come online duplexed because its database is out of date." (sideA or sideB)

Reason: This can happen when only one side of a duplexed system is upgraded. Loggers sideA and sideB must be at the same ICM versions

Solution: Follow steps outlined in ICM 7.2 Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.2(1)

Recommended Trace setting for Troubleshooting IPCC

The latest up-to-date recommended trace settings for troubleshooting in your IP Contact Center (IPCC) environment can be found on the web at: *http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_tech_note09186a0080094b22.shtml*.

Mobile Agent

Additional Trace Levels for Mobile Agent

Additional trace levels for troubleshooting Mobile Agent, in addition to those referenced in the previous section, are provided below:

JTAPI Gateway:

There is no separate trace mask for Mobile Agent. To enable trace for Mobile Agent, the following traces can be enabled as needed.

- Procmon <customer instance name> <nodename> jgw<#>
- >>>>trace JT_TPREQUESTS /on
- >>>>trace JT_CONNECTION /on
- >>>>trace JT_MEMORY /on

EAGTPIM:

There is no separate trace mask for Mobile Agent. The existing tele_drive_OP_ERR bit is turned on using default trace level.

CTIOS, CTISever, OPC:

There is no additional trace mask for Mobile Agent.

General Mobile Agent Troubleshooting

Condition: The user has configured the mobile agent option within the ICM Agent Desk settings page. However the Agent Desktop softphone application does not display any fields on the login dialog for the agent to log in as a mobile agent.

Problem: The CTIOS Server was not set up properly during install or the connection profiles defined in the registry are not defined correctly for Mobile Agents. The ShowFieldBitmask value needs to be defined in the connection profile for the appropriate mobile agent settings.

The CTIOS Server connection profiles sent to the CTIOS client desktop contains the information for ShowFieldBitmask which controls what fields are displayed on the login dialog.

Recommended Action: Rerun the CTIOS Server setup program, on the Peripheral dialog screen select the Mobile Agent option and the appropriate work mode. The registry is automatically updated with the appropriate values when the CTIOS Server setup program is run.

Condition: The agent is unable to select a call mode on the login dialog. The call mode field is disabled and set to either call-by-call or nailed connection without the option to change it.

Problem: The agent work mode needs to be set to "agent chooses" in order to be able to select the agent call mode.

Recommended Action: Rerun the CTIOS Server setup program and select "agent chooses" as the agent work mode on the Peripheral Identifier screen. Mobile Agent also needs to be selected in order to select the call mode. The registry is automatically updated with the appropriate values when the CTIOS Server setup program is run.

Condition: Call-by-call delivery to mobile agent fails and agent is logged out

Problem: Agent call cannot connect due to an invalid phone number.

Recommended Action: Check to make sure mobile agent phone number is entered correctly in the phone number field of the agent login UI before logging back in.

Condition: Call-by-call delivery to mobile agent fails and agent is set to not ready

Problem: Agent call cannot connect due to mobile agent phone line busy.

Recommended Action: Check agent phone line and make sure line is available.

Conditions:

- Nailed connection log in fails, AND "ConnFailedEv with cause of RESOURCE_NOT_AVAILABLE" in the JGW log, OR
- Call-by-call Mobile Agent call fails, AND "ConnFailedEv with cause of RESOURCE_NOT_AVAILABLE" in the JGW log

Problem: Call cannot connect due to codec mismatch.

Recommended Action: Check corresponding voice gateway codec configuration to match the codec setup in PG

Condition: Login failed: IPCC Error [10151] You haven't configured or have misconfigured the LCP Port on CCM Admin. Login denies. Invalid or missing LCP Port.

Problem: Unable to log into device due to an incorrect LCP configuration in CCM.

Recommended Action: Check the phone configuration page in CCM. Make sure that the device name of the LCP port starts with "LCP"

Condition: Login failed: IPCC Error [10152] You haven't configured or misconfigured the RCP Port on CCM Admin. Login Denied. Invalid or missing RCP Port.

Problem: Unable to log into a device due to an incorrect RCP configuration in CCM.

Recommended Action: Check the phone configuration page in CCM. Make sure that the device name of the RCP port starts with "RCP" and also check the device name of the corresponding LCP port.

Condition: Login failed: IPCC Error [10153] Mobile agent mode doesn't match the agent desk settings. Login Denied. Mobile agent mode is not allowed.

Problem: The agent's desk setting is not configured properly. Either mobile agent is not enabled or the agent work mode does not correspond to the agent call mode selected in the login dialog.

Recommended Action: Enable the mobile agent setting in the agent's desk setting. Verify that the agent mode configured in the agent's desk setting is the same as the agent call mode selected in the login dialog.

Condition: Login failed: IPCC Error [10154] Try to log in CTI PORT device for non-mobile agent or invalid CTI PORT for mobile agent. Login Denied. Agent is not allowed due to incorrect device.

Problem: A local agent is not allowed to log into a CTI port. Or if an invalid CTI port is used for login by a mobile agent.

Recommended Action: For a local agent, enter the agent's IP phone extension in the "instrument" field of CTI Login dialog box. For a mobile agent, check the CTI port configuration.

Samples of Mobile Agent Log Content

Agent login - When a mobile agent with agentID:2025 and remote phone number:2090 logs in using assigned local CTI port:5000, the "AgentInstrument" field will contain "5000;2090":

```
16:18:23 SESSION 1: MsgType:SET_AGENT_STATE_REQ (InvokeID:0xa0a5 PeripheralID:5000
AgentState:LOGIN
16:18:23 SESSION 1: AgentWorkMode:RA_NAILED_CONNECTION NumSkillGroups:0 EventReasonCode:0
16:18:23 SESSION 1: AgentInstrument:"5000;2090" AgentID:"2025" AgentPassword:"2025" )
```

An agent event is sent to the agent desktop. The "AgentInstrument" field in all subsequent agent events for that mobile agent with agentID:2025 has 5000 (aka, local CTI Port) as AgentExtension and AgentInstrument:

```
16:18:28 SESSION 1: MsgType:AGENT_STATE_EVENT (MonitorID:0 PeripheralID:5000 SessionID:0x0
16:18:28 SESSION 1: PeripheralType:EnterpriseAgent SkillGroupState:LOGIN StateDuration:0
16:18:28 SESSION 1: SkillGroupNumber:9577 SkillGroupID:5000 SkillGroupPriority:0
AgentState:NOT_READY
16:18:28 SESSION 1: EventReasonCode:0 MRDID:1 NumTasks:0 AgentMode:0 MaxTaskLimit:0
ICMAgentID:13910
16:18:28 SESSION 1: AgetAvailabilityStatus:0 ClientSignature:"CTIOSServer" AgentID:"2025"
16:18:28 SESSION 1: AgentExtension:"5000" AgentInstrument:"5000" )
```

Failed agent login - Try to log in a mobile agent (cti port=5001, remote phone=3000, agentID=74003) and agent's desk setting is set to Mobile Agent, but CTI Port Name for 5001 in CCM does not start with "LCP". Peripheral Error Code: PERERR_TELDRIVE_MOBILEAGENT_INCORRECT_LCP=10151:

```
11:19:54 SESSION 1: MsgType:SET_AGENT_STATE_REQ (InvokeID:0x6e78 PeripheralID:5000
AgentState:LOGIN
11:19:54 SESSION 1: AgentWorkMode:RA_NAILED_CONNECTION NumSkillGroups:0
EventReasonCode:50004 ForcedFlag:0
11:19:54 SESSION 1: AgentInstrument:"5001;3000" AgentID:"74003" )
11:19:54 Trace: ProcessSetAgentStateRequest - sessionID 1
11:19:54 Trace: *** AddToAssociateAgentList(); ADDED: SessionID=1 AgentID=74003
PeripheralID=5000
11:19:54 Trace: CSTASetAgentState - InvokeID=0x2a00f71b
     Device=5001;3000 AgentMode=LOG_IN AgentID=74003
```

```
     AgentGroup=-1(0xffffffff) AgentPassword=)
11:19:54 Trace: PrivateData - EventReasonCode=50004 WorkMode=0 NumAdditionalGroups=0
               PositionID= SupervisorID= ClientAddress=
11:19:54 Trace:
11:19:54 Trace: DEVICE_TARGET_OTS_IND - Instrument= Out-Of-Service NetworkTargetID=-1
11:19:54 SESSION 1: MsgType:SYSTEM_EVENT (PGStatus:NORMAL CCTimestamp:0x43d2e9e5 (01/21/06
21:11:49)
11:19:54 SESSION 1: SystemEventID:Agent Instrument Out-of-Service SystemEventArg1:0x1388
11:19:54 SESSION 1: SystemEventArg2:0xffffffff SystemEventArg3:0x0
EventDeviceType:DEVID_NONE )
11:19:54 Trace:
11:19:54 Trace: CSTAUniversalFailureConfEvent - InvokeID=0x2a00f71b
     Error=GENERIC_UNSPECIFIED_REJECTION
11:19:54 Trace:      PRIVATE_DATA - PeripheralErrorCode=0x27a7(10151)
11:19:54 SESSION 1: MsgType:CONTROL_FAILURE_CONF (InvokeID:0x6e78
FailureCode:CF_GENERIC_UNSPECIFIED_REJECTION
11:19:54 SESSION 1: PeripheralErrorCode:10151 )
```

Failed agent login - Try to log in a mobile agent (cti port=5001, remote phone=3000, agentID=74000) while agent's desk setting is not enabled for Mobile Agent. Peripheral Error Code: PERERR_TELDRIVE_MOBILEAGENT_MODE_NOT_ALLOWED=10153:

```
11:12:53 SESSION 1: MsgType:SET_AGENT_STATE_REQ (InvokeID:0x6dd4 PeripheralID:5000
AgentState:LOGIN
11:12:53 SESSION 1: AgentWorkMode:RA_NAILED_CONNECTION NumSkillGroups:0
EventReasonCode:50004 ForcedFlag:0
11:12:53 SESSION 1: AgentInstrument:"5001;3000" AgentID:"74000" )
11:12:53 Trace: ProcessSetAgentStateRequest - sessionID 1
11:12:53 Trace: *** AddToAssociateAgentList(); ADDED: SessionID=1 AgentID=74000
PeripheralID=5000
11:12:53 Trace: CSTASetAgentState - InvokeID=0x2a00f6ad
     Device=5001;3000 AgentMode=LOG_IN AgentID=74000
     AgentGroup=-1(0xffffffff) AgentPassword=)
11:12:53 Trace: PrivateData - EventReasonCode=50004 WorkMode=0 NumAdditionalGroups=0
               PositionID= SupervisorID= ClientAddress=
11:12:53 Trace:
11:12:53 Trace: CSTAUniversalFailureConfEvent - InvokeID=0x2a00f6ad
     Error=GENERIC_OPERATION_REJECTION
11:12:53 Trace:      PRIVATE_DATA - PeripheralErrorCode=0x27a9(10153)
11:12:53 SESSION 1: MsgType:CONTROL_FAILURE_CONF (InvokeID:0x6dd4
FailureCode:CF_GENERIC_OPERATION_REJECTION
11:12:53 SESSION 1: PeripheralErrorCode:10153 )
```

Mobile agent transitions to Available state - Mobile agent with agentID:2025 and remote phone number:2090 logged in using local CTI port(5000) sends a request to change its agent state to AS_AVAILABLE.

```
16:18:30 SESSION 1: MsgType:SET_AGENT_STATE_REQ (InvokeID:0xa0bb PeripheralID:5000
AgentState:AVAILABLE
```

```
16:18:30 SESSION 1: AgentWorkMode:RA_CALL_BY_CALL NumSkillGroups:0 EventReasonCode:0
AgentInstrument:"5000"
16:18:30 SESSION 1: AgentID:"2025" )
```

An agent event is sent to the agent desktop. Agent event has local CTI Port (5000) as AgentExtension and AgentInstrument.

```
16:18:30 SESSION 1: MsgType:AGENT_STATE_EVENT (MonitorID:0 PeripheralID:5000 SessionID:0x0
16:18:30 SESSION 1: PeripheralType:EnterpriseAgent SkillGroupState:AVAILABLE
StateDuration:0
16:18:30 SESSION 1: SkillGroupNumber:9577 SkillGroupID:5000 SkillGroupPriority:0
AgentState:AVAILABLE
16:18:30 SESSION 1: EventReasonCode:0 MRDID:1 NumTasks:0 AgentMode:1 MaxTaskLimit:1
ICMAgentID:13910
16:18:30 SESSION 1: AgentAvailabilityStatus:1 ClientSignature:"CTIOSServer" AgentID:"2025"
16:18:30 SESSION 1: AgentExtension:"5000" AgentInstrument:"5000" )
```

Note If a mobile agent is configured to use nailed connection, disconnecting the nailed connection call causes agent state to transition to AS_LOGGED_OUT.

Documentation Updates

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

Documentation Availability

The documentation for ICM/IPCC Enterprise and Hosted Editions Release 7.2(1) is available from http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

In particular the following is available through the above URL:

- Documentation for ICM/IPCC Enterprise and Hosted Editions Release 7.2(1)
- Documentation for System IPCC Enterprise Release 7.2(1)
- Documentation for CTI OS Release 7.2(1)
- Documentation for CAD Release 7.2(1)

The Cisco ICM/IPCC Release 7.2(1) documentation and the System IPCC Enterprise Release 7.2(1) documentation contain Release 7.2(1), 7.1(1), and 7.0(0) documents as follows:

- Documents labeled as 7.2(1) are provided because they include information that is new and specific to Release 7.2(1)
- Documents labeled as 7.1(1) include no new information specific to Release 7.2(1); however, if there is no 7.2(1) version of a document, a 7.1(1) version applies equally to both 7.1(1) and 7.2(1) releases.

- Documents labeled as 7.0(0) include no new information specific to Release 7.2(1) or 7.1(1); however, if there is no 7.2(1) or 7.1(1) version of a document, a 7.0(0) version applies equally to 7.0(0), 7.1(1), and 7.2(1) releases.
- In short, for 7.2(1)
  - use a 7.2(1) version of a document if it is provided
  - if not, use a 7.1(1) version of a document if it is provided
  - if not, use a 7.0(0) version of a document

Additional Documentation

This section contains new documentation that may not be available in the documentation set at the time of release.

Cycling PG After Changing Agent ID

If you change the Agent ID (Peripheral ID), you must cycle the PG in order to populate the new agent ID and information in the CTI OS Supervisor Desktop.

Enabling Mobile Agent in System IPCC

The online help page for configuring mobile agent in System IPCC mentions the need to check the 'Enable Cisco Unified Mobile Agent' check box in the 'Edit Desk Setting' page and choose the 'Mobile agent mode' from the drop down box.

However, it does not mention that you then need to re-run the CTI OS Server setup.

If CTI OS Server setup is not re-run at the end of the procedure currently described in the online help, Mobile Agent will not be enabled.

For a discussion of CTI OS Server setup and Mobile Agent, see the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise and Hosted Edition, Release 7.2(1).*

Outbound Option: Disabling Ringback During Transfer to Agent

In order that customers not hear a ringback tone while a call is being transferred to an agent, configure as follows:

Step 1 Log into the CallManager Administration window

Step 2 Access Service Parameters for CallManager

Step 3 Change "Send H225 User Info Message* " = "Use ANN for Ringback"

Step 4 Click **Update**

Step 5 Access Service Parameters for Cisco IP Voice Media Streaming Application

Step 6 Change, under "Annunciator (ANN) Parameters", "Run Flag" = "False"

Step 7 Click **Update**

Outbound Option: PortThrottleCount

The *Outbound Option Setup and Configuration Guide* has incorrect values for PortThrottleCount when deploying with Unified CallManager.

The table and notes in Chapter 2, "Installing/Configuring ICM Software for Outbound Option on IPCC Enterprise," Step 26, are incorrect.

The text should be as follows:

In the Dialer registry key, configure the Dialer throttling on each Dialer in the system using the PortThrottleCount and PortThrottleTime values.

PortThrottleCount indicates the number of ports to throttle and PortThrottleTime indicates the amount of time (in seconds) to throttle them.

For example, a count=10 and a time=2 indicates that no more than 5 calls can be started during a 1 second period. If 5 calls are ready to be dialed, they will be spaced evenly over that 1 second period.

The total call capacity of Unified CallManager is dependant on several different factors including: the version of Unified CallManager, the inbound call rate, and the outbound call rate. Please refer to the *Cisco Unified Contact Center Enterprise Solution Reference Network Design (SRND)* for details.

Note Without proper throttle settings it is possible for the Dialer to make too many calls, thereby overloading Unified CallManager and putting it into a Code Yellow condition.

WebView: Formula Given for TasksOffered in Caltyp22

In the WebView online help, the following formula is currently given:

```
Tasks offered (Call_Type_Half_Hour.CallsOfferedHalf) =
RouterCallsAbandQToHalf + ErrorCountToHalf + ICRDefaultRoutedToHalf +
CallsHandledHalf + OverflowOutHalf + IncompleteCallsHalf +
ShortCallsHalf + NetworkAnnouncementToHalf + ReturnBusyToHalf +
ReturnRingToHalf+ NetworkDefaultRoutedToHalf + ReturnReleaseToHalf +
CallsRONAToHalf + CallRoutedNonAgentToHalf
```

The correct formula is Completed Tasks (which should balance with CallsOfferedHalf in the Call_Type_Half_Hour table).

```
Completed Tasks = sum(isnull(CTHH.CallsHandledHalf,0))
          + sum(isnull(CTHH.TotalCallsAbandToHalf,0))
          + sum(isnull(CTHH.IncompleteCallsHalf,0))
          + sum(isnull(CTHH.ReturnBusyToHalf,0))
          + sum(isnull(CTHH.ReturnRingToHalf,0))
          + sum(isnull(CTHH.ICRDefaultRoutedToHalf,0))
```

```
+ sum(isnull(CTHH.NetworkDefaultRoutedToHalf,0))
+ sum(isnull(CTHH.OverflowOutHalf,0))
+ sum(isnull(CTHH.CallsRONAToHalf,0))
+ sum(isnull(CTHH.ReturnReleaseToHalf,0))
+ sum(isnull(CTHH.CallsRoutedNonAgentToHalf,0))
+ sum(isnull(CTHH.ShortCallsHalf,0))
+ sum(isnull(CTHH.AgentErrorCountToHalf,0))
+ sum(isnull(CTHH.ErrorCountToHalf,0))
```

ICM ID Finder Tool

Release 7.1(1) introduced additional support for the ICM ID Finder Tool. That additional support is documented here.

About the ICM ID Finder Tool

The ICM ID Finder is a tool that allows configuration managers and administrators to find the various configuration IDs of the following ICM components:

- Agent
- Label
- NIC
- Peripheral
- PG
- Physical Interface Controller
- Routing Client
- Service
- Service array
- Skill group
- Skill targets
- Translation route
- Application Path

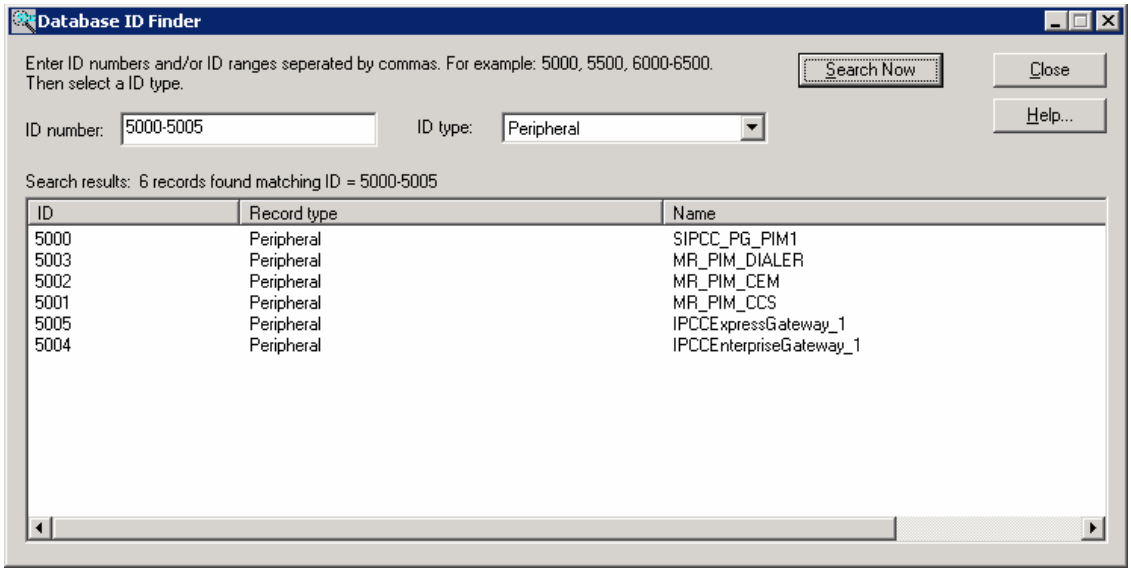
The ICM ID Finder tool helps you easily search for the IDs for particular ICM components. You can identify the component ID, record type and the name of the component from the search results by entering an ID or range of IDs.

Most of the ICM configuration tools do not show component IDs in the user interface; you need to look for the component IDs while setup or during configuration.

For System IPCC also, the ID Finder tool can be used for identifying the component IDs.

The user interface of this tool is shown in the following figure.

Figure 1 The ICM ID Finder Tool



Usage of the ICM ID Finder

The ICM ID Finder tool is used mainly in the following three cases:

- During ICM setup, the peripheral ID is required to setup a PG. The ICM ID Finder tool enables you to access the peripheral IDs.
- The ICM logs usually list the component IDs. During troubleshooting, the ICM ID Finder tool can be used to look for the object names by component IDs.
- In System IPCC, you do not see the component IDs. The ICM ID Finder tool helps you to get the component IDs whenever necessary.

How to Access the ICM ID Finder Tool

The ICM ID Finder tool is available as an executable file, idfinder.exe, starting in ICM version 4.6.2.

You can access this tool from all ICM Admin Workstations from the following path *icm\bin\idfinder.exe*.

In Release 7.1(1), the ICM ID Finder tool was enhanced to provide the ICM application path of the component ID.

How to Use the ICM ID Finder Tool

To use the ICM ID Finder tool, perform the following steps:

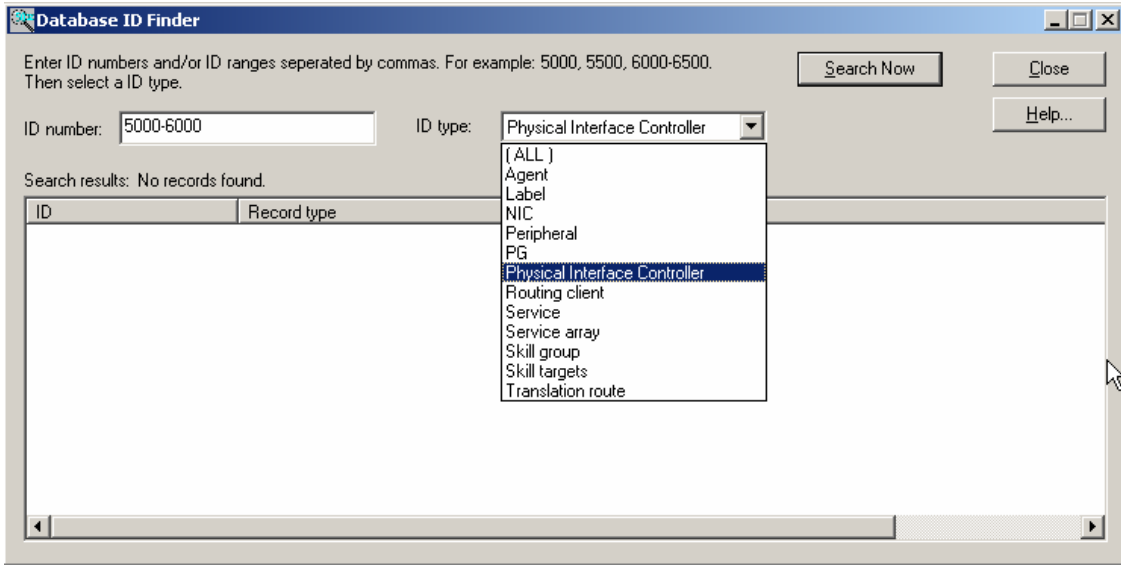
Step 1 Go to ICM > Bin.

Step 2 Double-click on the file idfinder.exe. The ID Finder screen opens up.

Step 3 Enter the ID range (such as 5000-6000) in the ID Number.

Step 4 Select the ID Type (such as Agent, Label) from the list, as shown in the figure below:

Figure 2 ICM ID Finder Tool: ID Types



Step 5 Click **Search Now** to get the results.

Note You can double click the column headers to sort the list.

Step 6 Click Close to close the ID Finder window.

Modifying the Skill Groups per Agent Limit

ICM and IPCC impose a default limit on the number of skill groups that can be assigned to a single agent (see Configuration Scalability Limit Enhancements, page 7). Once this limit is reached, additional skill groups cannot be assigned. The default limit is specified in the *IPCC Enterprise Solutions Reference Network Design Guide (SRND)*. The limit considers the total of both skill groups and sub-skill groups.

Note Also see Failure Occurs when Agent with 50 Skills Logs In on Child IPCC System, page 20.

If desired, you can use the ConfigLimit Tool to specify your own limit on the number of skill groups that can be assigned to an agent. For optimum performance, you can specify a limit far lower than the system default (see the SRND for performance considerations in choosing a skill groups per agent limit).

Caution You can also use the ConfigLimit tool to exceed the system default. Exceeding the default value for skill groups per agent can adversely affect system performance. Cisco will not support configurations that exceed the default value.

The ConfigLimit tool is a command-line tool utility from the bin directory of all ICM/IPCC Admin Workstations. Access is limited to users with privileges for the Setup or Config Groups in Active Directory for the chosen customer instance.

To change the skill groups per agent limit in configlimit.exe:

1. Launch a command line window on any Admin Workstation

2. Enter `configlimit`
3. Optionally, enter cl /show to view the existing limit
4. To change the limit, enter: `cl /id 1 value/<new_value> /update`

Example: `cl /id 1 value/5 /update`

5. Press Enter.

Lowering the Limit

If you have modified the skill groups per agent limit to be lower than the system default, no additional changes are necessary. The new, lower limit will be enforced immediately. Note that the new limit will NOT impact agents whose existing skill group membership exceeds the new limit until you next attempt to add a new skill group for those agents. At that time the new limit will be enforced, preventing you from adding additional skill groups.

Raising the Limit

If you have modified the skill groups per agent limit to be higher than the system default (in spite of the Caution given above), certain deployments will require the following additional changes to your system to use the new limit:

IPCC Gateway PG

For IPCC Gateway deployments, modify the following registry keys on your IPCC Gateway PGs to include the new value. A change to the registry will require that the PG service be restarted.

IPCC Enterprise Gateway PIM (IPCC Enterprise parent)

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\< customer_instance >\PG{n}[A|B]\PG\CurrentVersion\PIMS\pim{m}\ACMIData\Config\MaxSkills

IPCC Express Gateway PIM (IPCC Express parent)

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\< customer_instance >\PG{n}[A|B]\PG\CurrentVersion\PIMS\pim{n}\ACMIData\Config\MaxSkills

ERI PG

For ERI deployments, modify the following registry key on your ERI PGs to include the new value. A change to the registry will require that the PG service be restarted.

ER Service PIM

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\< customer_instance >\PG{n}[A|B]\PG\CurrentVersion\PIMS\pim{n}\ERSData\Config\MaxSkills

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

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML 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= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

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/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

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 submit comments about Cisco documentation 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.

Field Alerts and Field Notices

Note that Cisco products may be modified or key processes may be determined important. These are announced through use of the Cisco Field Alert and Cisco Field Notice mechanisms. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest. 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 will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—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 non emergencies.

- For Non emergencies—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 (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*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.html

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

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

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)—An existing 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 operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- 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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)