Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(3)

December 8, 2006

Contents

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

Introduction

ICM/IPCC Maintenance Release 7.1(3) supports ICM and IPCC Hosted & Enterprise Editions. This document discusses new features, changes, and caveats for Maintenance Release 7.1(3) of ICM/IPCC Enterprise and Hosted software.

This document is a supplement to the:

- *Release Notes for Cisco IPCC/ICM Enterprise & Hosted Editions Release 7.0(0) Installer Update C (28/Nov/2006)*
- *Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(1)*

Both can be found at:
http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_release_notes_list.html.

The ICM 7.1(3) Release Notes must be used in conjunction with both of the previously mentioned Release Notes. The latest version of this release can be found at:
http://tools.cisco.com/support/downloads/go/MDFTree.x?butype=cc

then:

Step 1 Click **Cisco Unified Contact Center Products**.

Step 2 Click **Cisco Unified Intelligent Contact Management Enterprise**.

Step 3 Click **Cisco Unified Intelligent Contact Management Software Releases.**

Step 4 Select the release you want then click the link to the desired release notes.

In addition, the CTI OS 7.1(3) Release Notes are available at:
http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod_release_notes_list.html.

About Release 7.1(3)

For all ICM Releases 7.1(2) and later, service releases (SR) are being renamed as maintenance releases (MR). Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(3) is the second maintenance release built on ICM Minor Release 7.1(1).

Maintenance Releases are cumulative updates to previous releases. As a result, applying Release 7.1(3) installs all the functionality contained in ICM 7.0(0) SR1 through SR4, 7.1(1) and 7.1(2), as well as the new 7.1(3) content. Due to this, ensure you read the relevant Release Notes prior to installing Release 7.1(3).

Release 7.1(3) can be installed over ICM/IPCC 7.0(0) FCS, 7.0(0) SR1 through SR4, 7.1(1) or 7.1(2).

ICM 7.1(3) also contains functionality delivered in Engineering Specials (ESs) built on ICM 7.0, 7.0 SR1 through SR4, 7.1(1), and 7.1(2) at least 60 days prior to the release date of 7.1(3). If your system has an ES installed whose functionality is not contained in 7.1(3), the installer displays a warning prior to performing any modifications to the system. The pre-7.1(3) ES must be uninstalled before the installation of 7.1(3) can be restarted.

For more information, and to obtain a replacement ES to be installed on the system after completing the SR4 installation, refer to the Cisco Bug Toolkit located at:
http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

The maintenance 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).

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/ps1001/prod_release_notes_list.html

About Cisco ICM and ICM Maintenance Releases

Cisco ICM software is a component of Cisco IPCC Enterprise, Cisco ICM Enterprise, Cisco ICM Hosted Edition and System IPCC Enterprise deployments. ICM maintenance releases deliver code updates that resolve issues in ICM software. They are made available as part of the ICM software maintenance strategy.

Maintenance releases for particular ICM versions are cumulative; they include code updates present in earlier minor, maintenance and service releases for their respective version. In the case of Release 7.1(3), the earlier minor release was Release 7.1(1).

ICM Maintenance Release 7.1(3) incorporates the following minor, maintenance, and service releases:

- Minor Release 7.1(1)
- Maintenance Release 7.1(2)
- Service Releases 7.0(0) SR1 through SR4

A Note about Product Naming

Cisco IPCC Enterprise Edition has been renamed to Cisco Unified Contact Center Enterprise (abbreviated as Unified CCE).

Cisco IPCC Hosted Edition has been renamed Cisco Unified Contact Center Hosted (abbreviated as Unified CCH).

These new names were introduced for Agent and Supervisor product opening-screens and in documentation that was revised for Release 7.1(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 Maintenance Release 7.1(3), 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.

Release 7.1(3) updates are also available for CTI OS. The CTI OS 7.1(3) Release Notes are available at: http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod_release_notes_list.html

See the *Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)* for information on agent desktop and PG software versions supported during 7.1(3) migration, as well as other important upgrade considerations.

ICM Version Support

ICM Maintenance Release 7.1(3) can only be installed on systems running Cisco ICM Releases ICM 7.1(1), ICM 7.1(2) or 7.0(0) SR1 through SR4. This includes ICM Enterprise Edition, ICM Hosted Edition, IPCC Enterprise Edition, IPCC Hosted Edition and System IPCC Enterprise deployments.

ICM 7.1(3) has been tested and verified to be compatible with the interoperability criteria for ICM Release 7.0(0). Additional ICM 7.0(0) interoperability support information is available from the following sources:

- ICM 7.0(0) support information for other Cisco products is listed in the *Cisco IP Contact Center Enterprise Edition Software Compatibility Guide*, available at: http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html.
- ICM 7.0(0) ACD support information is listed in the *ACD Supported Switch Matrix*, available at: http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/acddoc/index.htm.
- ICM 7.0(0) third-party platform support information is listed in the *Cisco ICM/IPCC Enterprise and Hosted Editions Release 7.0(0) Software and System Hardware Specifications (Bill of Materials)*, available at: http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm.
- Cisco Security Agent (CSA) for ICM, if used, must be the correct version. Support information is available at: http://www.cisco.com/kobayashi/sw-center/contact_center/csa/.
- The ICM release version on a PG must match the release version of CTI OS which is always co-resident. For example: a PG with ICM Release 7.1(3) requires CTI OS Release 7.1(3).

ICM Component Support

An ICM 7.0(0) maintenance release installs files that resolve caveats on different ICM 7.0(0) components. The installation program automatically detects the components installed on a machine and installs only those files specific to those components.

This section lists the ICM components on which this maintenance release can be installed, and those on which it cannot.

Supported ICM Components

ICM 7.1(3) is compatible with, and must be installed on, the following ICM components:

- ICM Administrative Workstations (AWs)
- ICM CallRouters
- ICM CTI Server
- ICM Historical Data Server
- ICM Loggers
- ICM Peripheral Gateways (PGs)

Note The ICM release version on a PG must match the release version of CTI OS which is always co-resident. For example: a PG with ICM Release 7.1(3) requires CTI OS Release 7.1(3).

- ICM Outbound Option Dialers
- ICM WebView Server
- System IPCC Enterprise Deployments

Note ICM 7.1(3) must be installed on all of the components listed above. Installing this maintenance release on only some of these components in an ICM system can result in inconsistent behavior in the ICM software.

ICM Components Unaffected by the Maintenance Release

There are no updates contained in the ICM 7.1(3) for the following components:

- Cisco Collaboration Server Dynamic Content Adapter (DCA)
- Cisco Computer Telephony Integration Object Server (CTI OS)
- Cisco E-Mail Manager Option (CEM)
- Cisco Media Blender (CMB)
- Cisco Web Collaboration Option (CCS)

It is not necessary to install this maintenance release on these machines unless a supported ICM component is co-located on them, in which case, the maintenance release must be installed.

New and Changed Information

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

Overview

Intelligent Contact Management (ICM) and IP Contact Center (IPCC) software Release 7.1(3) is a maintenance release that contains fixes and a limited set of new functionality. Release 7.1(3) is incremental and cumulative, and can be rolled back.

Release 7.1(3) introduces the following new feature:

- Agent Targeting Rules, page 7
- SEI-Lite (AAS Integration), page 8

New Features

Agent Targeting Rules

The Agent Targeting Rules allow you to configure ICM call routing by specifying the agent extension range, instead of configuring device targets and labels, for every phone and for every routing client. This simplifies the call routing configuration for the IPCC agent PGs.

The Agent Targeting Rules feature is supported for System PGs, CallManager PGs, and Generic PGs in IPCC Enterprise deployments (standalone IPCC Enterprise, IPCC Enterprise child of an ICM parent, or a CICM IPCC Enterprise in a NAM deployment).

Note The Agent Targeting Rules feature is not applicable, and is not required on System IPCC deployments.

You can define one or more rules for a peripheral. However, each rule must cover a different agent extension range for the same routing client. In other words, if there are multiple rules that a routing client can use to target a peripheral, there must be no overlapping extension ranges in those rules.

The following three rules can be used to route calls, depending upon the origin (routing client) and the destination (peripheral and agent extension) of the calls:

Agent Extension Rule

You can configure an Agent Extension Rule for routing calls from a routing client to a peripheral, that requires only the agent extension. The agent extension is acquired by the PG every time the agent logs in. The ICM CallRouter uses this rule as a default when the routing calls under the same peripheral.

Substitute Agent Extension Rule

You can configure a Substitute Agent Extension Rule for routing calls from a routing client to a peripheral that requires a prefix. This rule requires creating DID (Direct-Inbound-Dial) numbers for each agent logged in. This configuration is good for switches connected through inter-cluster trunks, and does not have limitations on the number of DIDs. While you can use the Substitute Agent Extension rule to route calls that are in the same peripheral, the Agent Extension Rule is more suitable. The ICM CallRouter creates a label containing the combination of a pre-defined prefix, plus the agent extension.

Translation Route Rule

You can configure a Translation Route Rule to route calls from a routing client to a peripheral that involves a translation route. The configuration allows you to reduce the number of DIDs required for routing. The ICM CallRouter creates a label consisting of a DID number that is shared to all calls, and that ICM translates to an agent extension using the translation route feature. A translation route configuration between the origin and destination needs to be configured before the configuration of this rule.

Configuring Agent Targeting Rules

You can configure Agent Targeting Rule by using a List tool, and it is available from the Configuration Manager by selecting either of the following:

- **Configure ICM > Targets > Device Target > Agent Targeting Rule**
- **Configure ICM > Tools > List Tools > Agent Targeting Rule**

To enable the Agent Targeting Rules, you need to select the *AgentTargetingMode* to "Rule Preferred" in the Advanced Tab of peripheral configuration of the PG Explorer.

You can find more information Agent Targeting Rules by going to ICM Configuration Tools on-line help:

- **Explorer Tools > PG Explorer > PG Property Descriptions > Agent Targeting Mode**
- **List Tools > Agent Targeting Rules**

Migrating Existing Device Target Routing to Agent Targeting Rules Routing

You can find information on migrating existing device target routing to agent targeting rule routing by going to ICM Configuration Tools on-line help:

- **Explorer Tools > PG Explorer > PG Property Descriptions > Agent Targeting Mode > Rules Compare to Existing Device Target**

Note Since the migration of existing device target routing to Agent Targeting Rules routing requires many manual steps as well as the testing of each device target and label covered by an agent targeting rule. This can be a substantial effort for large and complex configurations. To avoid this, continue using device target routing for existing PGs and use Agent Targeting Rules when installing new PGs.

SEI-Lite (AAS Integration)

The Automated Administrator for Symposium (AAS), from 7.1(3) onwards is included in ICM. With the inclusion of this component, now the AAS can be installed using the ICM installer. AAS patches will also be a part of ICM Service Release Installer. Refer to the install guide for installation of AAS Installing Automated Administrator for Symposium (http://www.cisco.com/application/pdf/en/us/guest/products/ps1001/c1097/ccmigration_09186a00805e8ccd.pdf).

ICM Maintenance Release Installation Planning

This section provides information to help you understand when to install an ICM maintenance release and the tasks it involves. It contains the following subsections:

When to Install an ICM Maintenance Release

Installing an ICM maintenance release requires temporarily stopping all ICM services and processes on your ICM components (Loggers, CallRouters, etc.). Therefore, to limit impact to a live ICM system, schedule and install ICM maintenance releases during a maintenance period when your ICM system is out of production.

Installation Order for ICM Components

ICM maintenance releases do not need to be installed on ICM components in a specific order. However, to avoid a temporary situation of mismatched components, install maintenance releases on the set of components comprising the Central Controller (CallRouter and Logger), Distributor, and Admin Workstation (Administration & WebView Reporting machines in System IPCC) at the same time. Patch Peripheral Gateways (Agent/IVR Controllers in System IPCC) as soon as possible after the Central Controller and Admin Workstation have been restarted.

Note The installation does require a specific order as it pertains to patching alternate sides of a duplexed ICM system. Consult How to Deploy ICM Maintenance Releases on a Duplexed ICM System, page 16 of this document for more information.

ICM Maintenance Release Installation Checklist

Deploying an ICM Maintenance Release requires the following general tasks:

- Schedule a maintenance period for installation: Because ICM maintenance release installation requires bringing down an ICM system, schedule maintenance release installation for a maintenance period when your ICM system is out of production.
- Determine which ICM components require maintenance release installation: Consult the “System Requirements” section of this document to determine on which ICM components this maintenance release must be installed.
- Inventory ICM nodes targeted for maintenance release installation: Take an inventory of all ICM nodes on which this maintenance release will be installed. If you are installing this maintenance release on a duplexed ICM system, consult How to Deploy ICM Maintenance Releases on a Duplexed ICM System, page 16 of this document for the correct order in which the installation must be applied to each side.

- Test and troubleshoot the installation: After installation, test your ICM system to ensure that it is working properly. Ensure that both sides of duplexed systems are synchronized by verifying that one side is active and the other side is idle. If desired, a failover test may be performed.
- Install the maintenance release on ICM nodes. Install the maintenance release on each Logger, CallRouter (Central Controller in System IPCC), Admin Workstation (Administration & WebView Reporting machine in System IPCC) and Peripheral Gateway (Agent/IVR Controller in System IPCC) in your ICM system. This section provides instructions on how to install ICM 7.1(3) and how to troubleshoot the installation.

Special Installation Instructions for International Customers

In order to generate correct ICM reports from WebView, some of the international customers need to perform additional steps before installing the maintenance release.

Important change to UK Customers

In ICM 5.0 and ICM 6.0, the default language for ICM created SQL login accounts was required to be set to "British English" on an UK platform.

In ICM 7.0, this requirement has been eliminated. Please do NOT change the default language for SQL login accounts created by ICM 7.0.

For UK and French Canadian Customers

French Canadian customers who prefer to use the European data format (dd/mm/yyyy) in their WebView reports should ignore this section.

The date display format needs to be adjusted for a Jaguar server installed on UK customers using the dd/mm/yyyy date format, or French Canadian customers using the yyyy/mm/dd date format.

For Danish Customers

Danish WebView server can be installed on either English or MUI version of Windows 2003 Server with Danish language pack. To view WebView report in dd/mm/yyyy format, the default language for IE Browser must be set to Dansk (da). See section “Default Language for IE Browser” on the language setting on IE Browser. See “Date Time in Jaguar Server” on how to adjust date time in Jaguar Server.

Default Language for IE Browser

The date format used by WebView is determined by the language setting in the IE browser. For example, if the language setting of the IE browser is en-us, WebView displays the date in mm/dd/yyyy format.

How to set the default language for IE browser

Step 1 In the IE browser, select **Tools > Internet Options …**, the Option dialog box appears.

Step 2 Click **Languages …** to add the appropriate language to the language list.

Step 3 UK English (en-gb) – the dd/mm/yyyy date format is used.

a. UK English (en-gb) – the dd/mm/yyyy date format is used

b. French (Canada) (fr-ca) – the yyyy/mm/dd date format is used

French Canadian customers who prefer to use the European data format (dd/mm/yyyy) in their WebView reports must use the default language (fr) in the IE browser.

Step 4 Move the newly selected language to the top of the language list.

Date Time in Jaguar Server

How to find the user name of the Jaguar server:

Step 1 On the desktop, right-click **My Computer**.

Step 2 Click **Manage** to bring up Computer Management window.

Step 3 In the left panel of the Management window:

a. Expand Services and Applications.

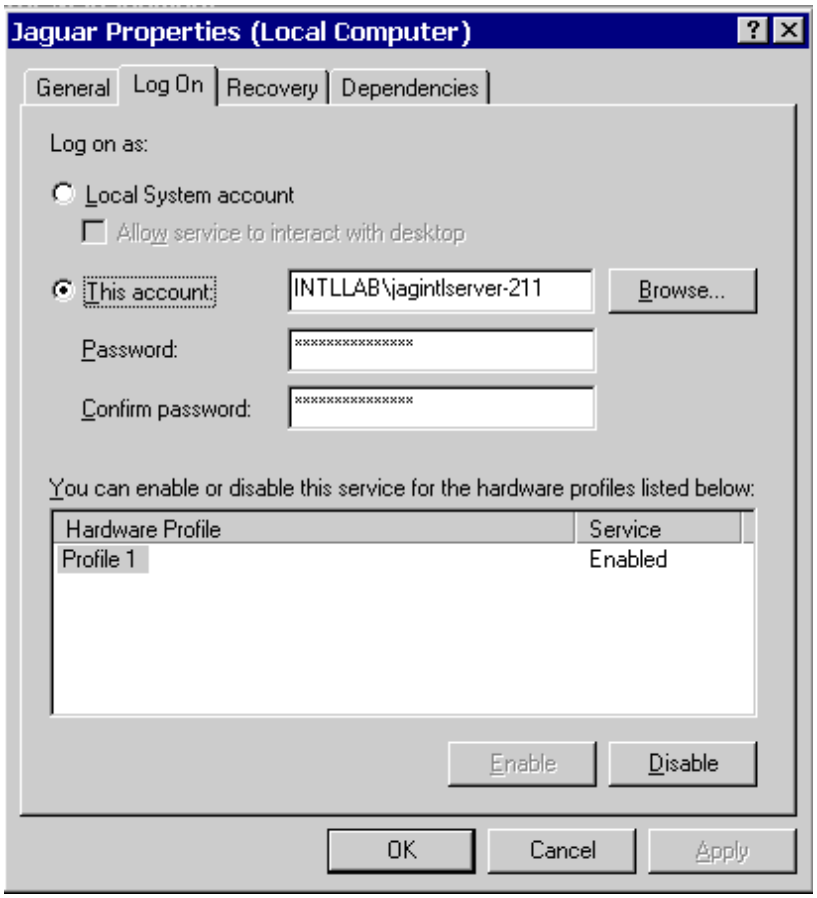
b. Click **Services**.

Step 4 In the right panel of the Management window:

a. Right-click **Jaguar**.

b. Click **Properties**, the Jaguar Propertie*s* dialog box appears.

Figure 1 Jaguar Properties Dialog Box



c. Select the **Log On** tab to obtain the user name of the Jaguar server (for example, jagintlserver-211).

How to find the Security ID (SID) of the Jaguar server user:

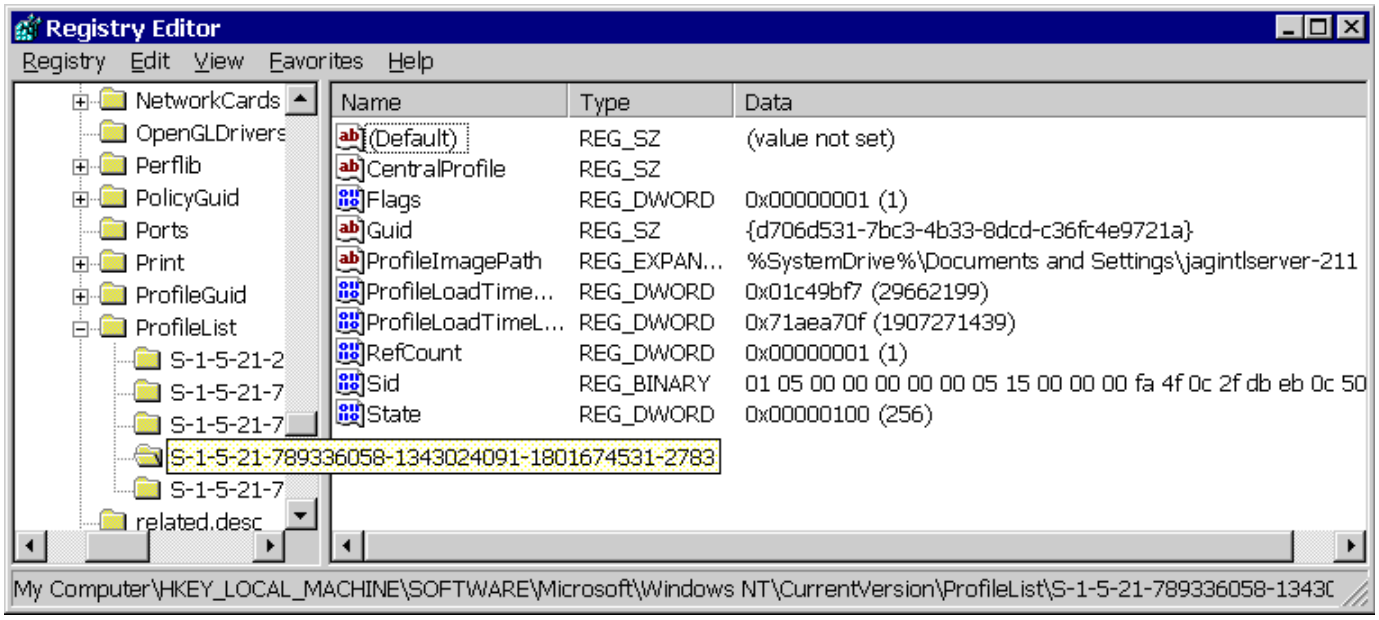
Step 1 Open **Start > Run**, enter **regedit**, and then click **OK**. The Registry Editor window opens.

Step 2 Open **My Computer/HKEY_LOCAL_MACHINE/SOFTWARE/MicroSoft/ windows NT/CurrentVersion/ProfileList**.

Note There is a list of sub-folders under this registry key. Open each of these folders, looking for the Jaguar server user name to appear in the Data column for the ProfileImagePath. The name of the folder in which the Jaguar server user name appears is the SID.

Step 3 Note the SID, especially the last digits. These digits differentiate the SID from the names of the other folders.

Figure 2 Regisry Editor



How to change the date format for Jaguar service:

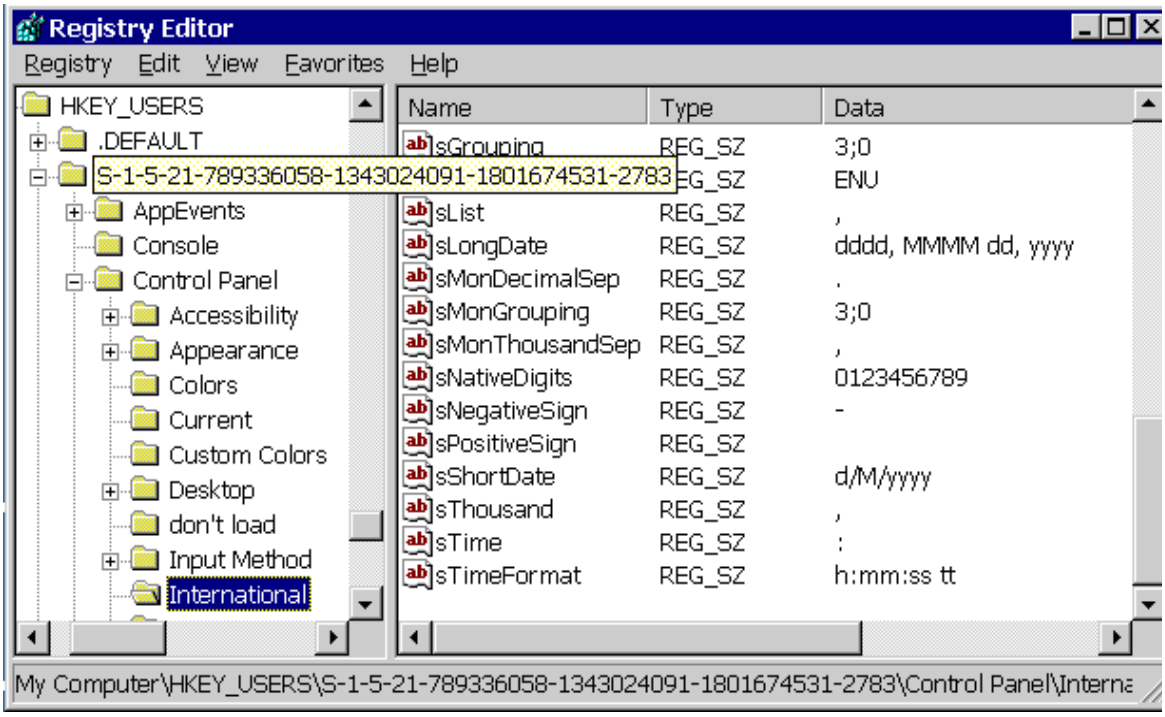
Step 1 In Registry Editor, go to **HKEY_USERS/ <SID of the user>/Control Panel/ International**. Double-click the **ShortDate** field. The Edit String dialog box appears.

a. Enter **d/M/yyyy** on a UK system.

b. Enter **yyyy/M/d** on a French Canadian system

c. Click **OK**. The following figure shows the correct date format on UK systems.

Figure 3 UK System Date Format



System IPCC Enterprise Deployment and Date Formats

If System IPCC is installed on French, German, or Spanish operating systems, the date format in the EAServer.ini file (pbodb100.ini) must be changed for WebView to be able to retrieve data correctly.

How 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.

Known Issues for International Customers

None.

Installation Notes

See the *Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)* for information on how to plan for and deploy Release 7.1(3).

Note The Install 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, or reboot the system.

This section provides important information to be read before installing the Release 7.1(3) update. For additional installation notes see the *Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)*.

Deploying ICM Maintenance Releases on a Duplexed ICM System

How to Deploy ICM Maintenance Releases on a Duplexed ICM System

If you are installing this maintenance release on a duplexed ICM system, you must install ICM maintenance releases on one side at a time, following the order described below:

Step 1 Install the maintenance release on all side A nodes following the steps described in the *Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)*.

Caution Do not restart ICM services on side A nodes at the completion of the installation.

Step 2 Stop all ICM and Cisco Security Agent (CSA) services on all side B nodes.

Step 3 Restart the ICM services on all side A nodes. Ensure the newly patched system is running with no errors in simplex mode.

Step 4 Once you have confirmed that side A is working correctly, install the maintenance release on side B nodes.

Step 5 Restart the CSA and ICM services on all side B nodes. Ensure both sides of the duplexed system synchronize.

System IPCC

For System IPCC, any servers with the following roles must use the same release of software (for example, Release 7.1(3)):

- Central Controller
- Administration and WebView Reporting
- Outbound Controller

For example, if you upgrade your Central Controller servers to Release 7.1(3), then you must upgrade your Administration & WebView Reporting servers and Outbound Controller servers to Release 7.1(3) as well. We also strongly encourage customers to keep their machines with "Agent/IVR Controller" roles (these servers have the IPCC System PG, CTI OS Server and CTI Server) at the same version as the Central Controller if they are on a separate server, and to keep their “Multichannel Controller” machine at the same version as the Central Controller.”.

Also, if after installing Release 7.1(3) you decide to roll back to Release 7.0(0) or 7.0(0) SR4, or Release 7.1(2), 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.

Release 7.1(3) removes Cisco Email Manager and Cisco Collaboration Server configuration components for Cisco Unified System Contact Center Enterprise. Integration with Cisco Email Manager and Cisco Collaboration Server was not supported, and the configuration components have been removed to reflect this.

Release 7.1(3) also contains modifications to the Cisco Unified System Contact Center Enterprise Multichannel Controller configuration that allows for integration with future Multichannel products.

The current Release 7.1(3) documentation does not reflect these changes. The help and documentation will be updated in a subsequent release. Also, if you have any Multichannel Controller machines configured in the System IPCC Web Administration (under **System Management > Machine Management > Machines**) they should be deleted before installing 7.1.3.

Running ICM Setup.exe in a Service and/or Maintenance Release Environment

This information is not applicable to System IPCC deployments. The following information pertains to ICM Releases 4.6(2) and above:

- Subsequent to an initial installation of ICM on a node, you may need to rerun Setup.exe from the ICM CD. Typically, this occurs when you want to add additional ICM components (loggers, CallRouters, etc.); this can only be accomplished by running the CD version of Setup.
- Potential issues can arise when the CD version of Setup.exe is run on ICM nodes on which service/maintenance releases and/or engineering specials have been applied. The CD version of Setup may overwrite files that were modified by the MR or ES installation. In ICM versions prior to 6.0, Setup.exe does not provide notification or warning of this potential risk.

Running ICM Setup.exe from the ICM CD in a Service and/or Maintenance Release Environment

To avoid potential issues, Cisco recommends that you revert an ICM node to the base-release level prior to running Setup.exe from the ICM CD. This must also be done if you have previously run Setup.exe from the CD in your service and/or maintenance release-patched environment and are experiencing inconsistent behavior.

How to run Setup.exe from the ICM CD in a service and/or a maintenance release environment

Step 1 Uninstall all ICM service releases, maintenance releases, and/or engineering specials from the node, following the uninstall instructions provided in their Release Notes.

Note Patches must be removed in the reverse-order they were installed. For example, on a node on which the following were installed, SR1 > SR1_ES10 > SR1_ES20 > SR4 > SR4_ES10 > SR4_ES20; you would remove patches in the following order: SR4_ES20 > SR4_ES10 > SR4 > SR1_ES20 > SR1_ES10 > SR1.

The un-installation program prevents you from removing patches in an incorrect order.

Step 2 Run Setup.exe from the ICM CD, adding components and/or making other configuration changes, as desired.

Step 3 After adding components and prior to exiting Setup, click Upgrade All to upgrade all ICM instances on the node.

Step 4 Reinstall ICM service releases, maintenance releases, and/or engineering specials, following the installation instructions provided in their Release Notes.

Recreate Service Account

The **Recreate Service Account** checkbox has been added to the Real-time Distributor Properties, the Logger Properties, and the WebView Node Properties dialog boxes.

Checking **Recreate Service Account** allows you to edit components without deleting and recreating the service accounts. This checkbox is only enabled when Local Setup is run to edit an existing instance. This checkbox is checked and disabled (grayed out) when installing a new instance using either Local or Media Setup.

When Local Setup is run to install an AW Distributor (with/without the Agent Re-skilling Web Tool enabled), a Logger, or WebView, it creates the service accounts by default, as needed. You do not have the option of disabling the creation of these service accounts.

When the ICM Media Setup is run to install an AW Distributor (with/without the Agent Re-skilling Web Tool enabled), a Logger, or WebView, it creates the service accounts. If the service account exists, then Setup deletes the existing service account, and recreates a new one. You are not given the choice to create, or not to create, the service account.

Limitations and Restrictions

Limitations and Restrictions are provided in the following documents:

- The *Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) and 7.1(2)* are available at: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_release_notes_list.html
- The *Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)*, updated for Release 7.1(3), available from http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm
- 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* (Updated for Release 7.1(1)) provides additional limitations and restrictions.

Release 7.1(3) is a cumulative update and may rectify restrictions as documented in the ICM Release 7.0(0) SR4, ICM 7.1(1) or ICM 7.1(2) Release Notes.

Important Notes

User List Tool Active Directory Issue

Symptom:

In a multiple domain scenario, the User List tool permissions checkboxes (Setup, Config and WebView) may not be checked. This is not a bug if all of the following are true:

- The deployment is split between two or more domains, such as the CICM and the Customer domain for Hosted customers
- The User List tool is used from two or more AWs that are in different domains
- The user is added via the User List tool on domain 1 and the retrieved via user list tool on domain 2

Cause:

The User List tool only scans the local domain (D1, the domain on which the tool is invoked) for ICM permissions. Since the ICM database is common to all AWs for an instance, if the User List tool is invoked from an AW in a different domain (D2), all users are displayed, but only permissions from the local domain (D1) are displayed. No permissions for the second domain (D2) are displayed because the users do not have permission(s) in that domain.

Solution:

None.

Caveats

Resolved Caveats in This Release

This section lists caveats specifically resolved by ICM 7.1(3). You can also find the latest resolved caveat information through the Bug Toolkit, an online tool available for you to query defects according to your own needs.

Caveats in this section are ordered by ICM component, severity, and then identifier.

Table 1 Resolved Caveats for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(3)

Identifier	Sev	Component	Headline
CSCse78316	6	aas	AAS Integration with ICM
CSCsf27706	3	aw.config	Created Skill group not visible to Agent
CSCse93475	3	aw.config	Default ATR Mode should be Rules Preferred for new peripherals
CSCse93547	3	aw.config	ATR Mode should be enabled while Generic (CallManager) PG is configured
CSCse87139	3	aw.config	User List doesn't properly show which ICM groups a user is a member of
CSCsg27536	3	aw.config	User List tool save operation is not efficient
CSCsg21458	2	ba.campaignmgr	CallbackNumber cannot be dialed due to leading 00s being removed
CSCse89437	2	ba.campaignmgr	Outbound campaigns apply Daylight Savings Time to all time zones
CSCse25560	3	ba.campaignmgr	Dialer may not attempt to contact a customer if Agents Skip or Reject
CSCse90270	2	ba.dialer	Dialer calls customer back if telcom temporary failure while talking
CSCse91133	3	ba.dialer	Outbound: Time to wait for available agent is 1sec longer than should be
CSCsg14165	3	ba.dialer	TransToIVR for answering machine causes repeat calls when should not
CSCse96015	6	ba.dialer	Dialer product doesn't support start and stop dates of DST in 2007
CSCse00026	3	ba.dialer.ipcc	Customer abandoned call during CPA is reported as Cancel-s/b abandoned
CSCse48445	3	ba.dialer.ipcc	Numbers not tried when campaign ended are not retried when restarted
CSCse78710	3	db.logger	UpdateRegions.exe changes not commited in DB
CSCsf04624	3	documentation	User List tool permissions checkbox not checked
CSCsf21165	4	documentation	Internal links in Agent Targeting Rule List Dialog Help throw an error
CSCse63775	2	inetscripted	Schedule Target config out of sync with internet script editor
CSCma22156	2	inetscripted	Cannot Save Script - Another user has changed the object
CSCse76668	2	inetscripted	ISE client synchronization intermittently stops
CSCse81593	3	inetscripted	Script lock is not released when ISE failed to save a script in QE mode
CSCma29821	3	inetscripted	Script lock is wrongly deleted in edit mode
CSCsg03742	3	inetscripted	Internet Script Editor crashes after saving a change
CSCsa87308	3	ipccinstall	Peripheral names (as they appear in ISE), unintuitive, mismatched.
CSCse83052	3	ipccwebconfig-ui	Can't create standalone AW when pointing to All-in-one

CSCse77387	3	ipccwebconfig-ui	System IPCC WebConfig shld provide choice for Mobile Agent CODEC
CSCsc18913	1	nic.crsp	CRSPNic crashes when receiving unexpected RunScript from Router
CSCse16836	3	nic.icrp	ICRPnic - CLI Presentation Restricted Indicator is not set by NIC
CSCsg26866	3	nic.inrcengine	NIC crash if RC taken offline with new route request in progress
CSCsg12884	3	nic.ss7innic	NoAnswerTimer encoding not controlled
CSCsd99833	3	patch	Error trying to copy non-existent WV files during temporary rollback
CSCse15613	3	patch	Local setup erroneously reports dynamic reskilling already installed
CSCsg26106	3	pg	Update 2007 DST changes for all peripherals
CSCsg03865	1	pg.alcatel	Alcatel Pim Failure
CSCse64896	6	pg.ars	QueryAgentStateMsg per agent needed
CSCsf01924	2	pg.definity	UseTrunkOverANIInCallingField option not availble in 6.0 for outbound ca
CSCse76746	2	pg.definity	ECSPIM crashes with DrWatson Entry ecspim!CVBridge::ProcENAlert
CSCma11734	6	pg.definity	Add capture/playback to pim for CMS-less
CSCsa26280	6	pg.definity	Performance degradation (3rd Party) after reaching max association limit
CSCse48237	2	pg.dms100	DMSPIM is not updating the Skillgroup information to OPC in conf event
CSCsg26720	1	pg.eapim	Mobile Agent Login causes ICMP unreachable packets
CSCsg43233	2	pg.eapim	PIM Crashes if Agt Logs in With Incorrect Num of Digits for Ext
CSCsf19318	2	pg.eapim	Outbound Option Calls fail with Resource Limitation Rejection error
CSCse89642	3	pg.eapim	Agent configuration updates do not make it to active EA PIM
CSCsf13905	2	pg.eapim.jtapigw	Mobile Agent calls fail with JT_JTAPI_EVENT_USED trace turned off
CSCse97871	2	pg.eapim.jtapigw	Performance of multiinstance PG system degraded
CSCse70890	3	pg.eapim.jtapigw	RONA doesn't work if CBC mobile agent's remote phone line busy
CSCse08760	3	pg.eapim.jtapigw	Mobile agents must login again after CTIManager failover
CSCsf96785	3	pg.eapim.jtapigw	Nailed-Up Mobile Agent Login Succeeds even if call can't be nail up
CSCse98921	2	pg.opc	Calls routed to the wrong agents due to LAA mis-calculation
CSCsg31367	2	pg.opc	opc assertion - Call Clear Trunk crash
CSCse36359	2	pg.opc	OPC Process restarts couple of times and then starts up
CSCsd66024	3	pg.opc	PG RT data persistence too infrequent, possible affect to call routing
CSCsf02051	3	pg.opc	Agent skg Half Hour data missing for removed skill
CSCse79995	3	pg.opc	OPC asserts during state Transfer
CSCse75639	4	pg.spectrumpim	Spectrum PIM Traces ACD Message Type in Numeric form
CSCse86378	2	router	RTR asserts when translation route to service array is used in script
CSCsf06719	3	serviceability.snmp	Cisco SNMP Agent crash with mindump on multi instance logger
CSCsf98130	2	setup	Editing component in local setup slow due to recreating service account
CSCse94598	3	setup	Domain Manager gives error if Domain Admins group not in root OU groups
CSCsf96661	3	setup	Performance of multiinstance PG system degraded
CSCse83902	3	setup.aw	AW won't connect if fully qualified domain name used in setup
CSCsg33222	3	setup.pg	Rtr and PG QoS settings are overwritten with defaults after local setup
CSCse90795	3	setup.pim	peripheral ID only populated to A side not B side in the registry

CSCse36650	3	setup.request.enh	ICM/IPCC Setup shld provide choice for Mobile Agent CODEC
CSCsf05925	3	setup.router	Real time feed cannot be established from Central Controller to AW/Dist
CSCse77797	3	setup.router	Router and PG Private QoS Settings not displayed correctly during setup
CSCsg59481	2	ipccwebconfig	Cannot modify or delete dialed numbers using System IPCC Web Admin

Bug Toolkit

How to access the Bug Toolkit

Step 1 Go to: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Step 2 Log on with your Cisco.com user ID and password.

Step 3 Click the **Launch Bug Toolkit** hyperlink.

Step 4 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 5 Click **Next**. The Cisco Unified Intelligent Contact Management Enterprise search window displays.

Step 6 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**.

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 7.1(3). Defects are listed by component and then by identifier.

If you have an account with Cisco.com, 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 2 Open Caveats for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(3)

Identifier	Component	Sev	Headline
CSCsg96801	ba.campaignmgr	3	2007 DST starts 6 days earlier for Pacific zone if LoggerA in - GMT bias
CSCsg85871	ipccwebconfig	2	Can't configure Network IVR in System IPCC after permanent uninstall
CSCsg84675	nic.incrp	2	Call fails intermittently with timeout error in NAM router.
CSCsg85257	pg.eapim.jtapigw	2	Mobile agents get logged out during load.

Documentation

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/ps1001/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 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

Additional Documentation

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

ICM ID Finder Tool

Release 7.1(1) introduced additional support for the ICM ID Finder Tool.

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

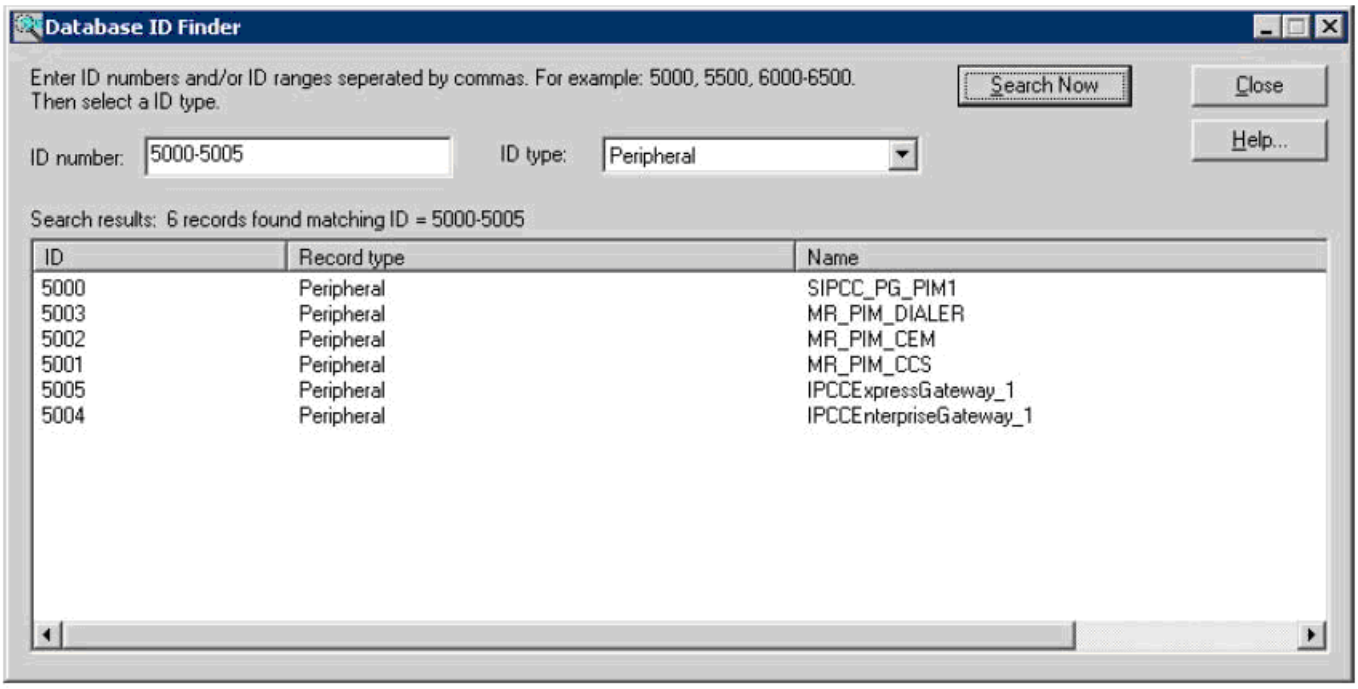
The ICM ID Finder tool helps you easily search for the IDs for particular ICM components. You can identify the component ID, record type and the name of the component from the search results by entering an ID or range of IDs.

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 4 ICM ID Finder Tool



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:

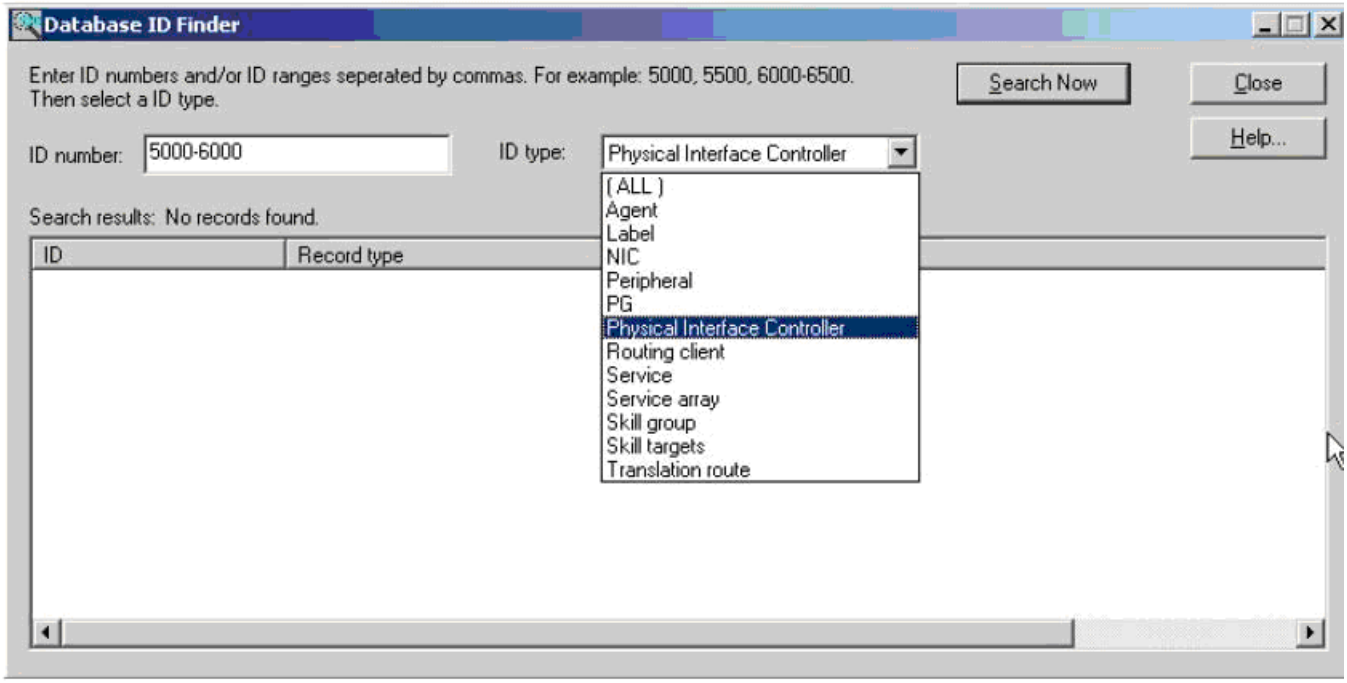
Step 1 **Step 1**Go to ICM > Bin.

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

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

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

Figure 5 ICM ID Finder: 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**, the ID Finder dialog box closes.

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: http://www.cisco.com/

You can access international Cisco websites at: 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: 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: 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: 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: 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: 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: 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: 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:

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: 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: 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: 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: 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: 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: http://www.cisco.com/go/iqmagazine, or view the digital edition at: 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.