

Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions

Release 7.1(5)

June 22, 2007

Contents

Introduction	3
About Release 7.1(5)	3
About Cisco ICM and ICM Maintenance Releases	4
A Note about Product Naming	4
System Requirements	5
ICM Version Support	5
ICM Component Support	5
Supported ICM Components	5
ICM Components Unaffected by the Maintenance Release	6
New and Changed Information	7
Overview	7
Configurable Route Trigger request in Siemens PIM	7
ICM Maintenance Release Installation Planning	8
When to Install an ICM Maintenance Release	8
Installation Order for ICM Components	8
ICM Maintenance Release Installation Checklist	8
Special Installation Instructions for International Customers	9
Important change to UK Customers	9
For UK and French Canadian Customers	9
For Danish Customers	9
For Dutch Customers	9
Default Language for IE Browser	12
Date Time in Jaguar Server	12
System IPCC Enterprise Deployment and Date Formats	16
Known Issues for International Customers	16
Installation Notes	17
Deploying ICM Maintenance Releases on a Duplexed ICM System	17
System IPCC	17

Running ICM Setup.exe in a Service and/or Maintenance Release Environment	18
Running ICM Setup.exe from the ICM CD in a Service and/or Maintenance Release Environment	18
Recreate Service Account	19
Limitations and Restrictions	20
Important Notes	21
Caveats	22
Resolved Caveats in This Release	22
Bug Toolkit	24
Open Caveats in This Release	25
Documentation	26
Related Documentation	26
Additional Documentation	26
ICM ID Finder Tool	26
Obtaining Documentation	28
Cisco.com	28
Product Documentation DVD	29
Ordering Documentation	29
Documentation Feedback	29
Field Alerts and Field Notices	30
Cisco Product Security Overview	31
Reporting Security Problems in Cisco Products	31
Obtaining Technical Assistance	32
Cisco Technical Support & Documentation Website	32
Submitting a Service Request	32
Definitions of Service Request Severity	33
Obtaining Additional Publications and Information	34

Introduction

ICM/IPCC Maintenance Release 7.1(5) supports ICM and IPCC Hosted & Enterprise Editions and System IPCC. This document discusses new features, changes, and caveats for Maintenance Release 7.1(5) 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)
- Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(2)
- Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(3)
- Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(4)

These release notes can be found at:

<http://tools.cisco.com/support/downloads/go/Platform.x?softwareType=Cisco%20Unified%20Intelligent%20Management%20Software%20Releases>

The ICM 7.1(5) Release Notes must be used in conjunction with the previously mentioned Release Notes.

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(5) Release Notes are available at:

<http://tools.cisco.com/support/downloads/go/Platform.x?softwareType=Cisco%20Computer%20Telephony%20Integration%20Software%20Releases>

About Release 7.1(5)

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(5) is the fourth 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(5) installs all the functionality contained in ICM 7.0(0) SR1 through SR4, 7.1(1), 7.1(2), 7.1(3), and 7.1(4), as well as the new 7.1(5) content. Due to this, ensure you read the relevant Release Notes prior to installing Release 7.1(5).

Release 7.1(5) can be installed over ICM/IPCC 7.0(0) FCS, 7.0(0) SR1 through SR4, 7.1(1), 7.1(2), 7.1(3), or 7.1(4).

ICM 7.1(5) also contains functionality delivered in all known Engineering Specials (ESs) built on ICM 7.0, 7.0 SR1 through SR4, and 7.1(1) through 7.1(4) that were released at least 60 days prior to the release date of 7.1(5). If your system has an ES installed whose functionality is not contained in 7.1(5), the installer displays a warning prior to performing any modifications to the system. The pre-7.1(5) ESs must be uninstalled before the installation of 7.1(5) 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 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(5), the earlier minor release was Release 7.1(1).

ICM Maintenance Release 7.1(5) incorporates the following minor, maintenance, and service releases:

- Minor Release 7.1(1)
- Maintenance Releases 7.1(2) through 7.1(4)
- 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(5), 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(5) updates are also available for CTI OS. The CTI OS 7.1(5) 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)* (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_installation_guides_list.html) for information on agent desktop and PG software versions supported during 7.1(5) migration, as well as other important upgrade considerations.

ICM Version Support

ICM Maintenance Release 7.1(5) can only be installed on systems running Cisco ICM Releases ICM 7.1(1) through 7.1(4), 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(5) 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(5) requires CTI OS Release 7.1(5).

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(5) 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(5) requires CTI OS Release 7.1(5).

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

 **Note** ICM 7.1(5) 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(5) 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(5) is a maintenance release that contains fixes. Release 7.1(5) is incremental and cumulative, and can be rolled back. The following new functionality is included in this release:

- [Configurable Route Trigger request in Siemens PIM](#)

Configurable Route Trigger request in Siemens PIM

The Siemens ACD has a necessary component called Route Trigger that is required for post routing and translation routing purposes. With the inclusion of this new feature, now the Customers can control the Route trigger being sent from PIM based on whether they are planning to use post/translation-routing or not.

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
- Installation Order for ICM Components
- ICM Maintenance Release Installation Checklist

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.



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 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 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(5) 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.

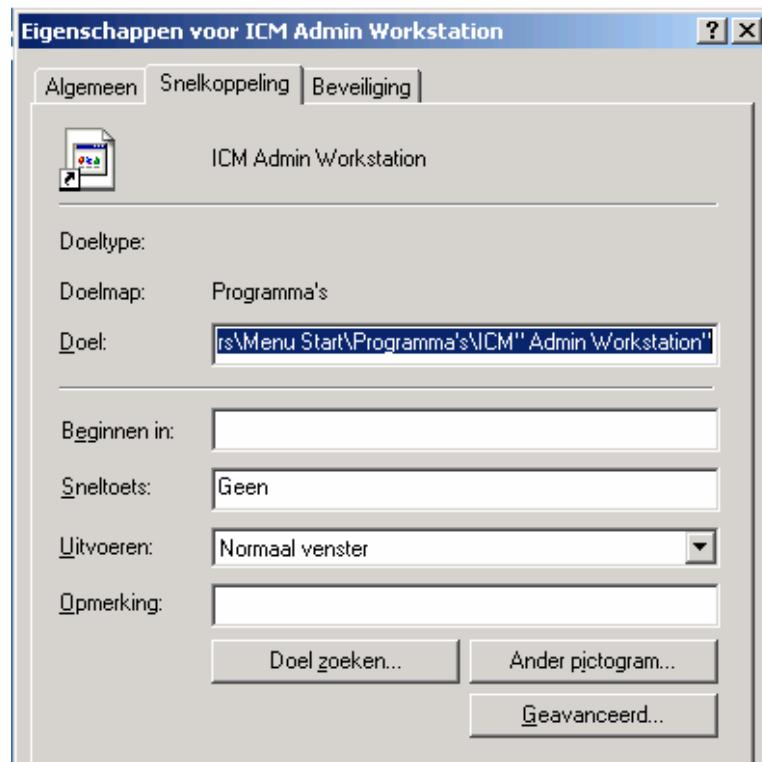
For Dutch Customers

Due to the 3rd party software ICM used, the link to AW program group icon appeared on the desktop of Dutch Windows 2003 Server is broken. It looks like:



To fix this, perform the following steps:

- Step 1** Right-click the incorrect AW program group icon, then select **Properties**. The Property dialog appears.



- Step 2** Click **Change Icon...** on the Property dialog.

- Step 3** When the warning message appears, click **OK**. The Change Icon dialog appears.



- Step 4** Select the program group icon high-lighted in the image above.
- Step 5** Click **OK**, to select the icon, then click **OK** to exit from the Properties dialog.
The AW program group icon now appears as follows.



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

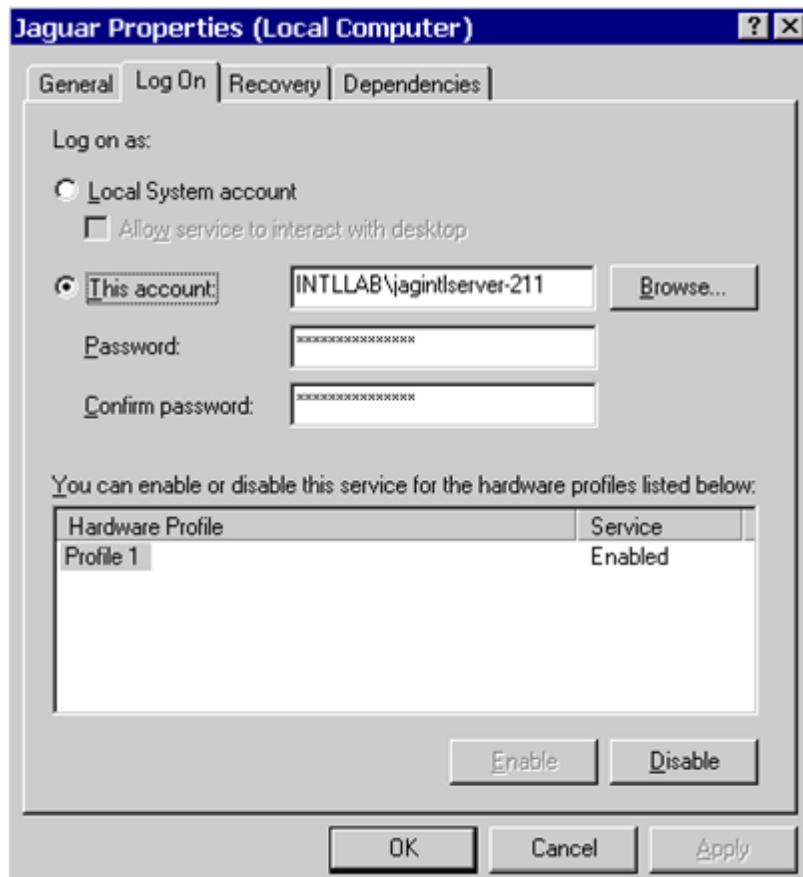
-
- Step 1** In the IE browser, select **Tools > Internet Options ...**, the Option dialog box appears.
 - Step 2** Click **Languages ...** to add the appropriate language to the language list.
 - Step 3** UK English (en-gb) – the dd/mm/yyyy date format is used.
 - a. UK English (en-gb) – the dd/mm/yyyy 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 Properties 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.

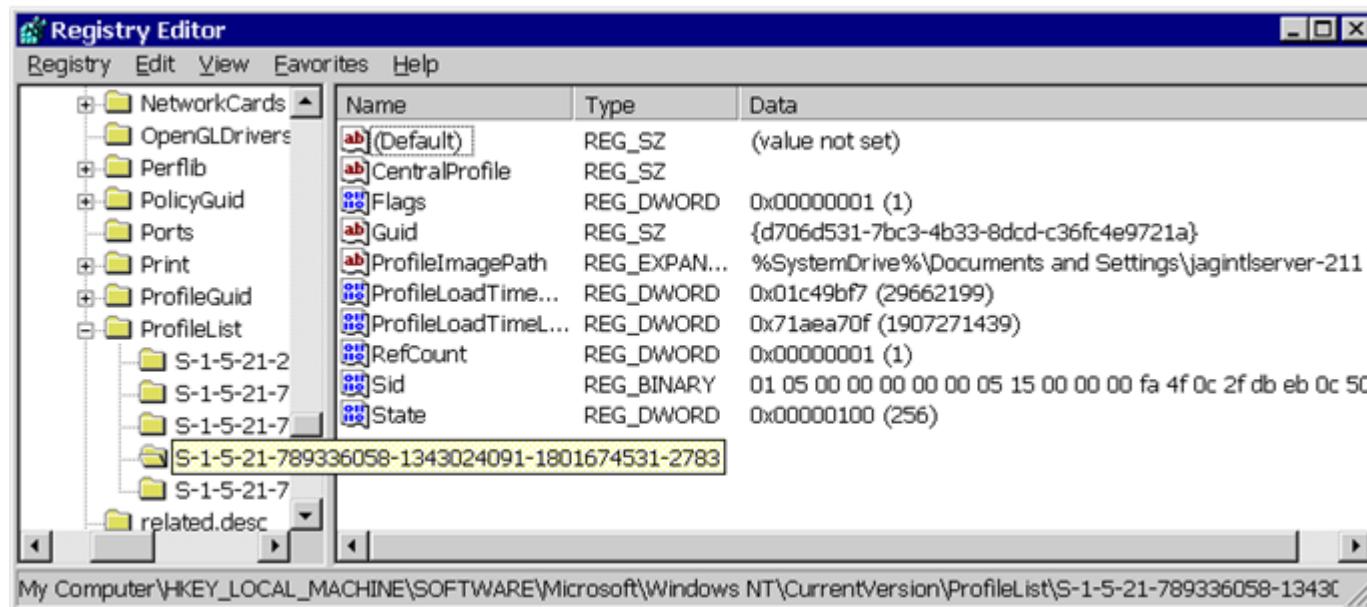
Step 2 Open My Computer/HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/windows NT/CurrentVersion/ProfileList.



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.

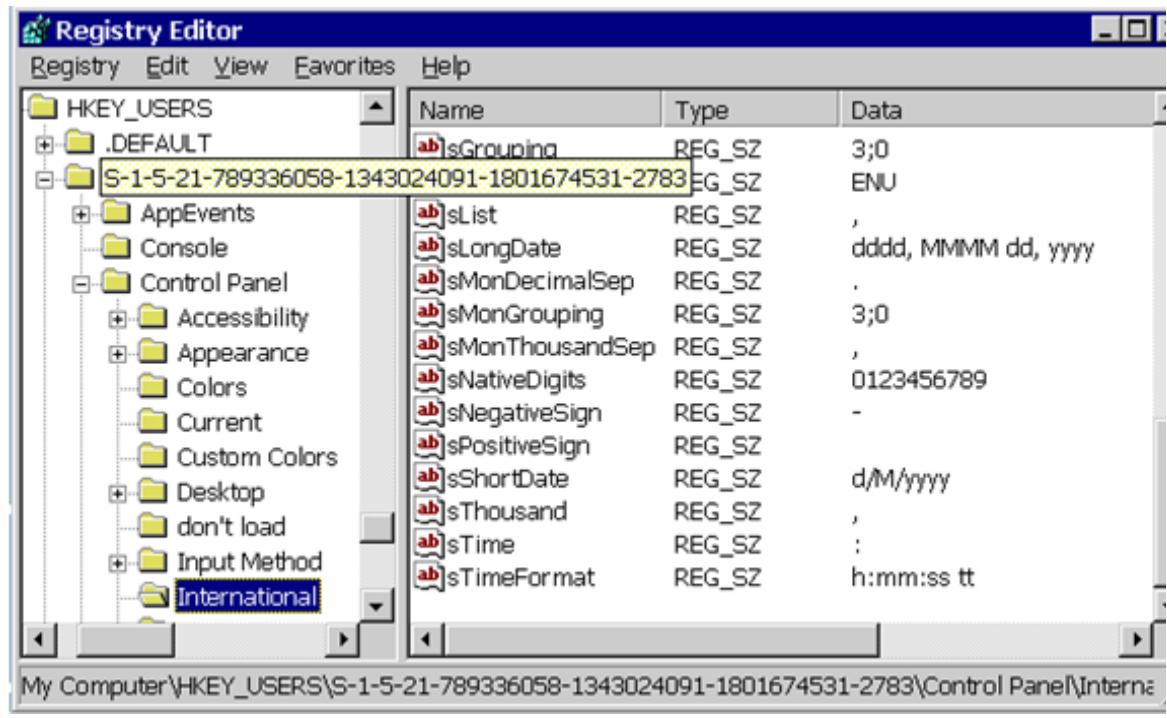
Figure 2 Registry Editor



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.
- Enter **d/M/yyyy** on a UK system.
 - Enter **yyyy/M/d** on a French Canadian system
 - 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\EA Server\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(5).

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(5) update. For additional installation notes see the *Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)* located at:

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

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(5)):

- Central Controller
- Administration and WebView Reporting
- Outbound Controller

For example, if you upgrade your Central Controller servers to Release 7.1(5), then you must upgrade your Administration & WebView Reporting servers and Outbound Controller servers to Release 7.1(5) 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(5) you decide to roll back to Release 7.0(0) or 7.0(0) SR4, Release 7.1(2), Release 7.1(3), or Release 7.1(4), 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(5) 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(5) 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(5) 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(5).

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(5), 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(5) is a cumulative update and may rectify restrictions as documented in the ICM Release 7.0(0) SR1 though SR4, and ICM 7.1(1) through 7.1(4) Release Notes.

Important Notes

None.

Caveats

Resolved Caveats in This Release

This section lists caveats specifically resolved by ICM 7.1(5). 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(5)

Identifier	Sev	Component	Headline
CSCsi26344	2	aas	CMSNode crashes when AAS makes request
CSCsi40222	3	aas	AAS doesn't use the local port specified in the registry AASConAPILocalP
CSCsh14300	3	aw.config	Agentcfg fails to add and delete a skillgroup member in single step
CSCsh40291	2	aw.config.explorer	Agent explorer takes a long time to display when agent selected
CSCsf09687	3	aw.synchronize	UAW crashing when processing a transaction
CSCsg43620	3	ba.campaignmgr	DoNotCall extensions which match an existing substring do not dial
CSCsi87974	2	ba.dialer	AutoAnswer feature on the dialer will not disable properly
CSCsi96637	2	ba.dialer	Unable to answer the Outbound call on Agent's device for G3 Dialer
CSCsh32124	6	ba.dialer	Dialer should only cancel customer calls that have not started ringing
CSCse94813	3	ba.dialer.ipcc	Invalid abandon route point config leaves call result as if successful
CSCsh31924	3	ba.dialer.ipcc	Outbound agent stays Ready for long time due to bad dialer port state
CSCsh67844	3	ba.dialer.ipcc	Dialer handles cancelled call while alerting as cancelled call result
CSCsh73875	3	ba.dialer.ipcc	Dialer handles no dial tone as cancelled
CSCsi15332	3	ba.dialer.ipcc	Dialer handles cancelled calls while alerting as customer abandoned
CSCsh77879	6	ba.dialer.ipcc	Dialer employs a bad logic to register dialer ports with standby CCM
CSCsc87886	3	cg.ctiserver	CTI Desktop doesn't show call/ECC Variables for BC on IPCC based setups.
CSCsi10417	3	cg.ctiserver	CTI Server sends messages for all Peripherals to its clients
CSCsb90386	3	db.distributor.realtime.feed	Some Skill Group Real Time Webview reports are lagging / not updating
CSCsg04089	2	db.distributor.rtf.client	rtclient exception on hosted icm distributor
CSCsi02001	2	db.distributor.rtf.client	rtdist write to client connection failed (rtclient)
CSCsf22395	3	db.icmdba	ICMDBA fails at startup -- SQL Server is unavailable or does not exist
CSCsi29672	3	localization	Webview French report perskg22 is missing column headers
CSCsh81341	3	nic.crsp	CRSPNicV3 fails to send all labels with multi-label support
CSCsh31341	3	nic.ss7innic	Dynamite: ICM responded TaskRefused with PAbort dropped call
CSCsh75456	3	nic.ss7innic	SS7IN NIC will abort NCT call on failure of SplitLeg operation
CSCsh75513	6	nic.ss7innic	Add ECC variable for on-hold treatment
CSCsg26106	3	pg	Update 2007 DST time for peripherals in time zone different from ACD
CSCsh71260	2	pg.acmi	ACMI: CAD can't get call data unless 'PermitApplicationRouting' enabled
CSCsg73106	2	pg.ars	(1339) PIM Crashes if Agt Logs in with extra digits prepended to Ext
CSCsh68910	2	pg.aspect	Aspect keep alives
CSCsi03590	2	pg.aspect	Agent Desktop Greys Out while making Agent state to ready.
CSCsh15628	3	pg.aspect	Agent PIM stops processing agent state data.
CSCsh15562	2	pg.definity	Agent is not able to clear an out bound call

CSCsh79921	2	pg.eapim	EA-PIM re-starts when agent logs in with a space pre-pending extension
CSCsh85324	2	pg.eapim	Unconfigured route points sometimes cause EAPIM to stop call processing
CSCsh35293	3	pg.eapim	Agent Stuck in talking if call is transferred from unmonitored device
CSCsh43588	3	pg.eapim	Wrapup timer cleared with transferred call
CSCsh67955	2	pg.eapim	Agent stuck in on hold state
CSCsh52164	2	pg.eapim.jtapigw	mobile agent hold function doesn't stop voice from agent to caller
CSCsi06971	2	pg.eapim.jtapigw	no voice path between mobile callbycal non-control SIP phone and customer
CSCsi09518	3	pg.eapim.jtapigw	CTIOS desktop comes up with error when transfer a transferred call
CSCsh33683	3	pg.eapim.jtapigw	Blind Transfer of conference of unmonitored devices does not work
CSCsh61133	3	pg.eapim.jtapigw	missing RTP Start on Conference for conferenced party
CSCsh98217	3	pg.eapim.jtapigw	Agent can't login after PG and CCM services recycle
CSCsi12523	6	pg.eapim.jtapigw	Mobile Agents hear Music on Hold during PG or Call Manager failover
CSCsh32188	2	pg.mrpim	High average agent available time if Release Call node in ICM script
CSCsh61408	2	pg.opc	Problems when large numbers of PGs all send their HH data simultaneously
CSCsh84709	2	pg.opc	Agent doesn't get calls when not ready in MR domain
CSCsi00243	2	pg.opc	Calls have wrong Peripheral Call Type in the Termination Call Detail
CSCsi10202	2	pg.opc	ARI transferring a call to VRU using translation route fails
CSCsi14998	2	pg.opc	OPC Asserted on both sides after Agent answered the call
CSCsg57385	3	pg.opc	OPC restarts if agent hangs up on supervisor asst after reskill (logged in)
CSCsh02628	3	pg.opc	Personal CallBack call from dialer can't be transferred to another agent
CSCsh56165	3	pg.opc	Unexpected error from OPI ReadNextUpdateElement in router log
CSCsi02123	3	pg.opc	Call variables lost during CG failover.
CSCsi35545	6	pg.siemens-rolm	Acquiring of Route Trigger to be made configurable in Siemens PG
CSCsh63110	2	pg.spectrumacd	Spectrum acd Agt xfer/confer calls missing TCD
CSCsg15869	2	pg.spectrumpim	Spectrum PIM gets Caught Exception and Crashes.
CSCsi25072	4	reporting	WebView - On Change Items unselected items are selected
CSCsa58679	2	reporting.webview	Unable to log into WebView- jagconnection.prop is deleted by WebView
CSCsh88278	2	reporting.webview	Exporting Real Time reports to HTMLTable produces blank page
CSCsi29694	4	reporting.webview	The caltyp23 report is not showing data in chronological order
CSCsh63301	2	router	Requery fails if call is sent to VRU after TransRouted to type2 VRU
CSCsh98646	2	router	Router crashes during state transfer
CSCsi24395	2	router	Router may go out of sync when there are calls queued during state transfer
CSCsi33069	2	router	CICM Router Crashed
CSCsi10483	2	security	Authenticating User logging into Webview fails due to time out
CSCsh79423	2	setup	Cannot start PG installed by local setup, on a CG only system
CSCsa44810	3	setup.pg	PG Setup doesn't retain the QoS Settings

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:
- 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.
 - 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.

- 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.

- 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.
- 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(5). 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(5)

Identifier	Component	Sev	Headline
CSCsi42776	aw.config.explorer	2	Trusted Domains do not appear in Agent Explorer list.
CSCsg85257	cp-mediacontrol	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

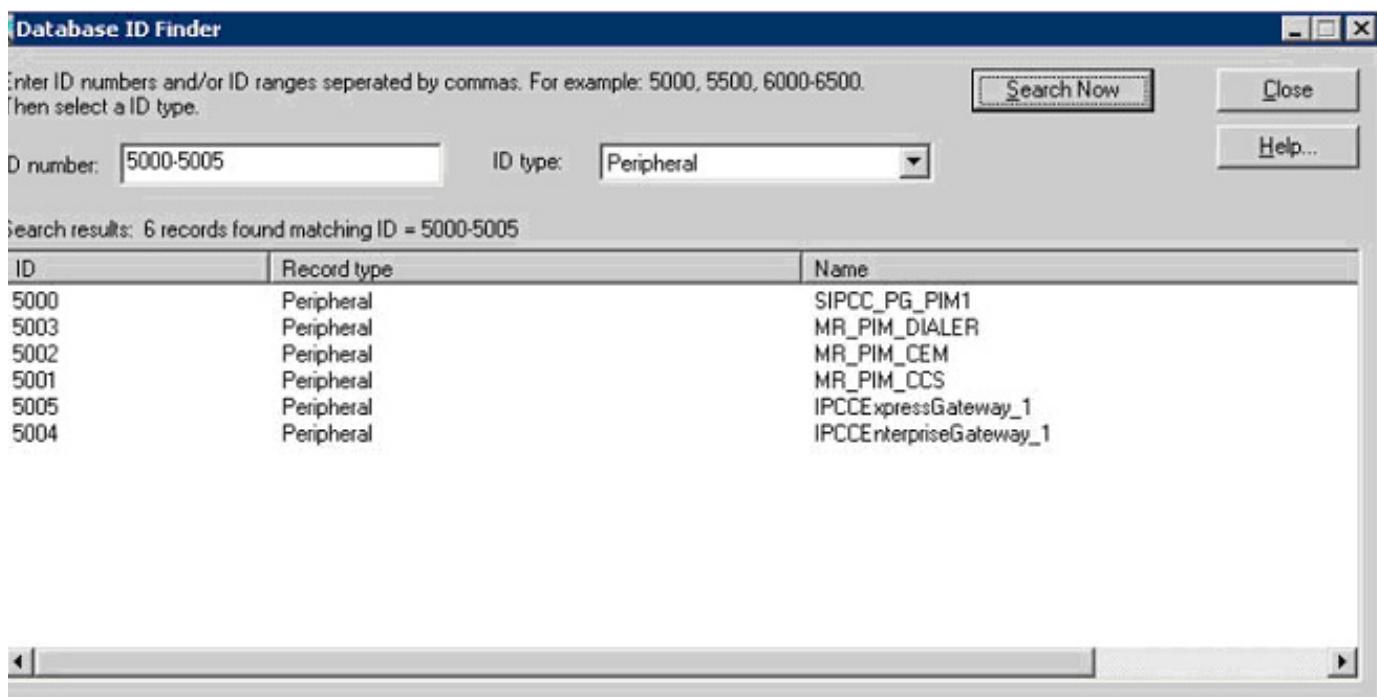
The ICM ID Finder tool helps you easily search for the IDs for particular ICM components. You can identify the component ID, record type and the name of the component from the search results by entering an ID or range of IDs.

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`.

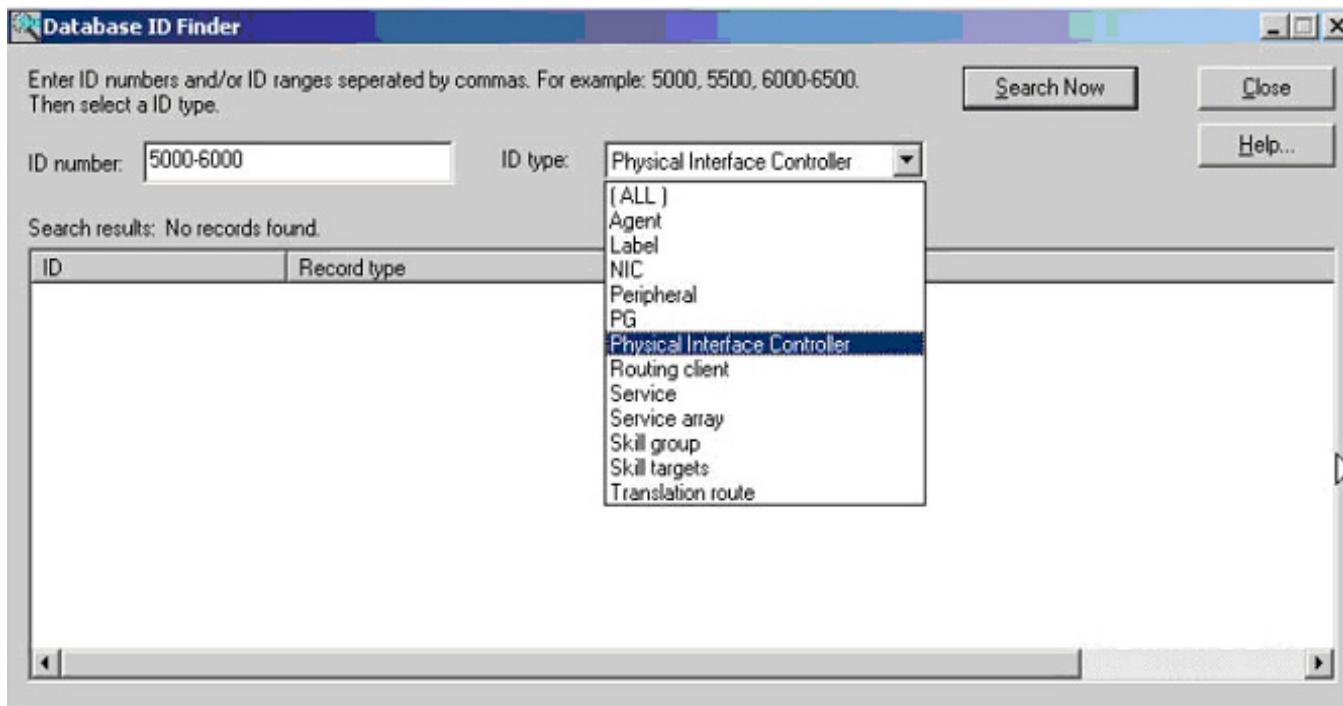
In Release 7.1(1), the ICM ID Finder tool was enhanced to provide the ICM application path of the component ID.

How to use the ICM ID Finder Tool

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

- Step 1** 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 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



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>.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, 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. (0612R)