System IPCC Enterprise Installation and Configuration Guide
Cisco IPCC Enterprise Edition
7.0(0)

May 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0833
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCBs public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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, 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. (0609R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Copyright © 2007 Cisco Systems, Inc. All rights reserved.
# Table of Contents

Preface ................................................................................................................................. 1
Purpose ................................................................................................................................. 1
Audience ............................................................................................................................ 1
Organization ....................................................................................................................... 1
Related Documentation...................................................................................................... 3
Conventions......................................................................................................................... 3
Obtaining Documentation................................................................................................. 4
  Cisco.com......................................................................................................................... 4
  Product Documentation DVD......................................................................................... 4
  Ordering Documentation................................................................................................. 5
Documentation Feedback.................................................................................................. 5
Product Alerts and Field Notices..................................................................................... 5
Cisco Product Security Overview....................................................................................... 5
  Reporting Security Problems in Cisco Products ............................................................. 6
Obtaining Technical Assistance........................................................................................ 7
  Cisco Technical Support & Documentation Website....................................................... 7
  Submitting a Service Request......................................................................................... 7
  Definitions of Service Request Severity......................................................................... 8
Obtaining Additional Publications and Information........................................................ 8

## Part 1. Product and Platform Information .................................................................... 11

1. Introduction to System IPCC Enterprise....................................................................... 13
   About IPCC Enterprise .................................................................................................. 13
   About System IPCC Enterprise Core Components...................................................... 13
   IPCC Enterprise Optional Software Components....................................................... 15
   Basic IPCC Call Flow................................................................................................... 16

2. IPCC Enterprise Platform Specifications.................................................................... 19
   About IPCC Enterprise Server Hardware Requirements.............................................. 19
   About IPCC Enterprise Operating System Requirements.......................................... 21
   About IPCC Enterprise Network and Active Directory Domain Requirements........ 21
      Supported Windows Active Directory Models......................................................... 21
   About IPCC Enterprise 3rd Party Software Requirements.......................................... 22
   About IPCC Internationalization and Localization Support...................................... 22
   About IPCC Enterprise Component Version Interoperability.................................... 22
   Licensing Requirements and System Limitations......................................................... 23
   About Non-Supported Component Features in an IPCC Environment....................... 23

3. System IPCC Deployment Models............................................................................... 25
   About System IPCC Deployment Models................................................................... 25
   Choosing A Deployment Model: Load Considerations............................................... 28

## Part 2. Installing and Configuring System IPCC Enterprise ...................................... 29

4. Overview of Installation and Configuration Tasks....................................................... 31
   Hardware Installation Checklist................................................................................... 31
   IPCC Enterprise Staging Requirements...................................................................... 32
   IPCC Enterprise Component Software Installation Checklist................................... 32
   IPCC Enterprise Component Software Configuration Tasks..................................... 34

5. Installing and Configuring Cisco CallManager for System IPCC Enterprise............. 35
How to Install Cisco CallManager for IPCC Enterprise .................................................. 35
CallManager Configuration Tasks .................................................................................... 36
About the CallManager Administration Utility .............................................................. 36
How to Configure Agent IP Phones for IPCC Enterprise ............................................... 37
  How to Configure IP Phones on the CallManager ....................................................... 37
  How to Set the Agent IP Phone Configuration on the IP Phone ............................. 38
About the CallManager Extension Mobility Feature ...................................................... 38
How to Configure CTI Route Points .............................................................................. 39
How to Configure CTI Ports ......................................................................................... 40
How to Configure JTAPI Users for the Agent/IVR Controller and IP IVR ...................... 41

6. Installing and Configuring Cisco IP IVR for IPCC Enterprise .................................... 43
About IP IVR .............................................................................................................. 44
About IP IVR Installation Prerequisites ........................................................................ 44
How to Install IP IVR for IPCC Enterprise ................................................................... 44
IP IVR Configuration Tasks ......................................................................................... 45
About the CRS Administration Utility ....................................................................... 46
How to Configure the Directory Profile ...................................................................... 46
How to Configure the JTAPI User on the IP IVR System ............................................. 48
How to Configure CTI Port Groups .............................................................................. 48
How to Configure the ICM Subsystem ........................................................................ 50
How to Configure and Upload VRU Scripts ............................................................... 50
About Translation Routing and Post Routing .............................................................. 51
How to Configure IP IVR for Translation Routing ....................................................... 52
How to Configure IP IVR for IPCC Post Routing ....................................................... 54
How to Configure and Start the Application Engine .................................................. 55
How to Verify and Update the JTAPI Client ............................................................... 55

7. Installing and Configuring the Controllers and Administration & WebView Reporting ................................................................. 57
3rd Party Software: Prerequisite Installations .............................................................. 57
3rd Party Software: Packaged Software ...................................................................... 58
Installation Guidelines................................................................................................. 59
Installing and Configuring the Controllers and Administration & WebView Reporting ................................................................. 59
Post-Installation Configuration: How to Configure Machines ................................... 62
About the IPCC Web Administration Tool Deployment Wizard .............................. 62
Initial Configuration: Machine Type Requirements .................................................. 63
How to Complete Deployment Wizard Pages .......................................................... 64
  Wizard Page: Describe your IPCC Deployment ....................................................... 64
  Wizard Page: Describe the IPCC Machine in your Deployment ............................ 64
  Wizard Page: IPCC Network Settings .................................................................... 65
  Wizard Page: Call Manager Connectivity Settings ............................................... 66
  Wizard Page: IVR Connectivity Settings .................................................................. 67
  Wizard Page: Database Settings ............................................................................ 68
Re-Accessing and Disabling the Deployment Wizard .................................................. 68
About Machine Roles .................................................................................................. 68
Post-Installation Configuration: Create Additional IVR Connections and Grant System Permissions ................................................................. 69
Post-Installation Configuration: Create Agents and Groups ..................................... 70
Post-Installation Configuration: Set Up Contact Routing ......................................... 71

8. Installing Agent and Supervisor Desktop Software for IPCC Enterprise ..................... 73
About Agent and Supervisor Desktops for IPCC Enterprise ....................................... 73
About the CTI Server and the CTI OS Server ............................................................ 74
About Agent and Supervisor Desktop Installation Prerequisites .................................. 74
How to Install CTI OS .......................................................................................................................... 75
  How to Install the CTI OS Supervisor Desktop ...................................................................................... 75
  How to Install the CTI OS Agent Desktop ............................................................................................... 76
How to Install and Configure the Cisco Agent Desktop Applications .................................................. 77
  Cisco Agent Desktop (CAD) Pre-Installation Requirements ................................................................. 77
  How to Install and Configure the Cisco Agent Desktop Applications .................................................. 80
9. Installing and Configuring Outbound Option for IPCC Enterprise ................................................... 83
   About Outbound Option ........................................................................................................................ 83
   How to Install Outbound Option for IPCC Enterprise ......................................................................... 84
   Outbound Option Configuration Tasks ................................................................................................. 84
   How to Configure Outbound Option Dialers ......................................................................................... 84
   How to Configure General System Time Options ................................................................................. 85
   How to Enable Call Variables for Outbound Option ........................................................................... 85
   How to Configure the Transfer to IVR Feature ...................................................................................... 86
   How to Configure CallManager for Outbound Option ........................................................................ 86
      How to Configure the Outbound Option Port Devices ...................................................................... 86
      How to Enable the CallManager Call Waiting Option on Outbound Agent Phones ...................... 87
      How to Configure Music on Hold ...................................................................................................... 87
   About Scripting for Outbound Option .................................................................................................. 88
      About the Outbound Control Variable ............................................................................................... 88
      About the Outbound Percent Variable ............................................................................................... 89
10. Installing and Configuring Cisco Multichannel Components for IPCC Enterprise ........................ 91
    About IPCC Enterprise Multichannel Components ........................................................................... 91
    About Cisco Collaboration Server ...................................................................................................... 91
    About Cisco E-Mail Manager ............................................................................................................. 92
    About Multichannel Installation Prerequisites .................................................................................. 92
    How to Install Multichannel Components for IPCC Enterprise ...................................................... 92
    About IPCC Configuration for Multichannel Components ............................................................... 93
       About Multichannel Controllers ...................................................................................................... 93
       About Media Routing Domains ...................................................................................................... 93
       About Multichannel Agents ............................................................................................................ 94
       About Multichannel Skill Groups .................................................................................................... 94
       About Application Instances (Multichannel Authentication) .......................................................... 95
       About Administration Connections ................................................................................................ 95
       About Universal Queue and Multichannel Routing Scripts ............................................................ 96
    How to Configure Multichannel Components for IPCC Enterprise ................................................. 97
       How to Modify Media Routing Domain Configuration ................................................................. 97
       How to Configure Application Instances ....................................................................................... 98
       How to Establish Administration Connections .............................................................................. 99
       How to Set Call Variables .............................................................................................................. 100
       How to Write IPCC Routing Scripts for Multichannel Options ..................................................... 101
       How to Configure Cisco Collaboration Server for IPCC Integration ......................................... 101
       How to Configure Cisco Media Blender for IPCC Integration ....................................................... 102
       How to Configure Cisco E-Mail Manager for IPCC Integration ..................................................... 102
11. Configuring Reporting for IPCC Enterprise ...................................................................................... 105
    About Reporting Configuration Prerequisites ................................................................................... 105
    IPCC Reporting Configuration Tasks .................................................................................................. 106
    How to Configure Service Levels ....................................................................................................... 106
       How to Modify the Global Service Level for Call Types ................................................................ 106
       How to Set Service Levels for Specific Call Types ......................................................................... 107
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>System IPCC Core Components</td>
<td>14</td>
</tr>
<tr>
<td>Figure 2</td>
<td>System IPCC Optional Components</td>
<td>15</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Basic IPCC Call Flow</td>
<td>17</td>
</tr>
<tr>
<td>Figure 4</td>
<td>System IPCC Deployment Topology</td>
<td>28</td>
</tr>
<tr>
<td>Figure 5</td>
<td>System IPCC Databases</td>
<td>122</td>
</tr>
</tbody>
</table>
Preface

Purpose

Welcome to the Cisco System IP Contact Center (IPCC) Enterprise Edition Installation and Configuration Guide. This guide provides information to help you understand, install, and configure the System deployment of IPCC Enterprise.

Audience

This guide is written for anyone who is responsible for installing, configuring, and maintaining a System IPCC Enterprise in a production or laboratory system, including network administrators, IPCC system administrators, and call center administrators.

Organization

This guide contains the following sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to System IPCC Enterprise</td>
<td>Provides a brief description of the IPCC Enterprise system and an explanation of its components.</td>
</tr>
<tr>
<td>IPCC Enterprise Platform Specifications</td>
<td>Provides hardware and software specifications for System IPCC Enterprise components. It also provides a list of component features not supported when components are deployed as part of a System IPCC Enterprise deployment.</td>
</tr>
<tr>
<td><strong>Section</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>System IPCC Deployment Models</td>
<td>Provides an overview of System IPCC supported deployments.</td>
</tr>
<tr>
<td>Overview of Installation and Configuration Tasks</td>
<td>Provides task checklists designed to help you track your progress as you install and configure IPCC.</td>
</tr>
<tr>
<td>Installing and Configuring Cisco CallManager for IPCC Enterprise</td>
<td>Describes how to install and configure Cisco CallManager software for System IPCC Enterprise.</td>
</tr>
<tr>
<td>Installing and Configuring Cisco IP IVR for IPCC Enterprise</td>
<td>Describes how to install and configure IP IVR software.</td>
</tr>
<tr>
<td>Installing and Configuring the Controllers and Administration &amp; WebView Reporting</td>
<td>Describes how to install and configure the IPCC Controllers and Administration &amp; WebView Reporting component.</td>
</tr>
<tr>
<td>Installing and Configuring Outbound Option for IPCC Enterprise</td>
<td>Describes how to configure the optional Outbound Option feature for System IPCC Enterprise.</td>
</tr>
<tr>
<td>Installing Agent and Supervisor Desktops for IPCC Enterprise</td>
<td>Describes how to install and configure Cisco Agent Desktop and CTI OS Agent Desktop and IPCC Supervisor Desktop.</td>
</tr>
<tr>
<td>Installing and Configuring Cisco Multichannel Components for IPCC Enterprise</td>
<td>Describes how to install and configure Cisco Multichannel software for System IPCC Enterprise.</td>
</tr>
<tr>
<td>Configuring Reporting for System IPCC Enterprise</td>
<td>Describes tasks required to configure reporting for your IPCC Enterprise system.</td>
</tr>
<tr>
<td>IPCC Troubleshooting</td>
<td>Provides troubleshooting information for IPCC installation, utilities, and use.</td>
</tr>
<tr>
<td>About System IPCC Enterprise Databases</td>
<td>Describes IPCC databases.</td>
</tr>
<tr>
<td>Uninstalling and Reinstalling IPCC</td>
<td>Describes how to uninstall and reinstall the IPCC controllers and Administration &amp; WebView Reporting machines.</td>
</tr>
<tr>
<td>Increasing Fault Tolerance in an IPCC Enterprise System</td>
<td>Provides information on how to configure IPCC Enterprise for fault tolerance.</td>
</tr>
<tr>
<td>System IPCC to Cisco ICM Component and Feature Comparison</td>
<td>Maps System IPCC terminology and functionality to its Cisco ICM counterparts.</td>
</tr>
</tbody>
</table>
Related Documentation

For additional documents and information about IPCC Enterprise and the System deployment of IPCC Enterprise, see the Cisco web page (http://www.cisco.com/univercd/home/home.htm).

Conventions

This manual uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example:</td>
</tr>
<tr>
<td></td>
<td>• Choose <strong>Edit</strong> &gt; <strong>Find</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Finish</strong>.</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Italic font is used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• To introduce a new term. Example: A <em>skill group</em> is a collection of agents who share similar skills.</td>
</tr>
<tr>
<td></td>
<td>• For emphasis. Example: <em>Do not</em> use the numerical naming convention.</td>
</tr>
<tr>
<td></td>
<td>• A syntax value that the user must replace. Example: IF (<em>condition</em>, <em>true-value</em>, <em>false-value</em>)</td>
</tr>
<tr>
<td></td>
<td>• A book title. Example: See the Cisco CRS Installation Guide.</td>
</tr>
<tr>
<td><strong>window font</strong></td>
<td>Window font, such as Courier, is used for the following:</td>
</tr>
<tr>
<td></td>
<td>• Text as it appears in code or that the window displays. Example: <code>&lt;html&gt;&lt;title&gt;Cisco Systems, Inc. &lt;/title&gt;&lt;/html&gt;</code></td>
</tr>
</tbody>
</table>
Convention | Description
--- | ---
< > | Angle brackets are used to indicate the following:
- For arguments where the context does not allow italic, such as ASCII output.
- A character string that the user enters but that does not appear on the window such as a password.

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:


Product Documentation DVD

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

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can register to receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information. Access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en.

Cisco Product Security Overview

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

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 and notices for Cisco products is available at this URL:

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

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


Reporting Security Problems in Cisco Products

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

- 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 nonemergencies.

- For Nonemergencies: psirt@cisco.com

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

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

Note: 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:

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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


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 Tools. Choose Cisco Product Identification Tool from the Alphabetical Index drop-down list, or click the Cisco Product Identification Tool 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 TAC engineer. The TAC Service Request Tool is located at this URL:

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Product Quick Reference Guide is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:
• Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

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

http://www.ciscopress.com

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

http://www.cisco.com/packet

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

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

• *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:


• 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:

Part 1: Product and Platform Information
About IPCC Enterprise

The Cisco IPCC Enterprise system functions as a virtual ACD. Some of the capabilities of IPCC include intelligent multichannel contact routing, ACD functionality, network-to-desktop computer telephony integration (CTI), interactive voice response (IVR) integration, call queuing, and consolidated reporting.

With IPCC Enterprise, the contact center manager can configure agents to handle inbound and outbound voice, Web collaboration, text chat, and e-mail requests. The agents can switch between those media on a task-by-task basis. Customers can choose the medium that is most comfortable and convenient for them. IPCC Enterprise can be used in a single-site environment or integrated into a multi-site contact center via Cisco's IPCC Gateway.

About System IPCC Enterprise Core Components

This section describes the core software components of the System IPCC Enterprise system. For more detailed information regarding software components and IPCC architecture, refer to the Cisco IP Contact Center Enterprise Edition Solution Reference Network Design Guide.

Core components of System IPCC include an Administration & WebView Reporting machine, a Central Controller, an Agent/IVR Controller, Cisco CallManager, and Cisco IP IVR. Reporting
is provided through WebView. Agent desktop functionality is provided through, optionally, CTI OS or Cisco Agent Desktop (CAD) software.

**Figure 1: System IPCC Core Components**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Controller</td>
<td>The Central Controller, the Agent/IVR Controller, and the Administration &amp; WebView Reporting components provide intelligent contact routing and ACD functionality, including monitoring and controlling agent state, CTI capabilities, and gathering real-time and historical data for reporting in the IPCC Enterprise system.</td>
</tr>
<tr>
<td>Agent/IVR Controller</td>
<td>The Central Controller provides system call routing and logging functionality. The Agent/IVR Controller provides communication link between the central controller and the Cisco CallManager and IP IVR. The Administration &amp; WebView Reporting component provides system administration/configuration and WebView reporting functionality.</td>
</tr>
<tr>
<td>Administration &amp; WebView Reporting</td>
<td></td>
</tr>
<tr>
<td>Cisco CallManager</td>
<td>Cisco CallManager provides features comparable with those of a traditional PBX system and handles the switching requirements of the IPCC system. It allows deployment of voice applications and the integration of telephony systems with Intranet applications.</td>
</tr>
<tr>
<td>Cisco IP IVR</td>
<td>Cisco IP IVR provides Interactive Voice Response (IVR) and queuing capability in the IPCC system.</td>
</tr>
</tbody>
</table>

Note: Based on your licensing, the IP IVR version you are running may be named “IP IVR” or “IP Queue Manager.” In either case, the instructions for deploying it with IPCC are the same. “IP IVR” is the term used throughout this guide.
Note: IPCC Enterprise does not support CRS clustering (duplexed IP IVRs that failover to the same CTI route points). System IPCC supports connections for up to five IP IVRs per Agent/IVR Controller. In deployments containing multiple IP IVRs, System IPCC's Network VRU automatically balances load across the IP IVRs based on trunk availability.

Cisco CTI Object Server (CTI OS) and Cisco Agent/Supervisor Desktop (CAD) are server-based CTI solutions that provide desktops used by contact center agents and supervisors. You select which of these applications to deploy with your IPCC system.

CTI OS includes the CTI OS Agent Desktop, IPCC Supervisor Desktop, CTI OS Toolkit, and Client Interface Library (CIL). Cisco Agent/Supervisor Desktop includes the Desktop Administrator, Agent Desktop, and Supervisor Desktop.

### IPCC Enterprise Optional Software Components

The following optional software components can be (but are not required to be) deployed in an IPCC Enterprise system. This group of components provide outbound dialing capability and Web and E-mail interactivity to IPCC. The Web and e-mail options are referred to collectively in IPCC Enterprise deployments as the Multichannel components.

*Figure 2: System IPCC Optional Components*

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound Controller</td>
<td>The Outbound Controller provides outbound dialing capability for the Outbound Option feature. It is required only if you are deploying Outbound Option. Outbound Option is a feature that provides outbound dialing functionality along with existing inbound capabilities of IPCC software. With Outbound Option, contact centers can be configured for automated outbound activities. Agents who are not busy handling inbound requests can perform outbound calls, thereby maintaining a high level of agent productivity.</td>
</tr>
</tbody>
</table>
## Basic IPCC Call Flow

The figure below shows the flow of a basic IPCC call. In this scenario, all of the agents are assumed to be "not ready" when the call arrives, so the call is routed by the System IPCC controller to the IP IVR. While the call is connected to the IP IVR, call queuing treatment (announcements, music, and so on) is provided. When an agent becomes available, the IPCC controller directs the IP IVR to transfer the call to that agent's phone. At the same time the call is being transferred, the IPCC controller sends the caller data such as Automatic Number Identification (ANI) and Directory Number (DN) to the agent desktop software.
The call flow shown above is as follows:

1. Call delivered from PSTN to voice gateway.
2. MGCP or H.323 Route Request sent to Cisco CallManager.
3. JTAPI Route Request sent to ICM.
4. ICM runs routing script. No available agent found, so ICM label returned from routing script.
5. ICM instructs Cisco CallManager to transfer call to IP IVR, and Cisco CallManager does as instructed.
6. IP IVR notifies ICM that call has arrived.
7. ICM instructs IP IVR to play queue announcements.
8. Agent becomes ready (completed previous call or just went ready).
9. ICM sends call data to selected agent screen and instructs the IP IVR to transfer the call to the agent phone.
10. IP IVR transfers the VoIP voice path to selected agent phone.
11. Call is answered by agent.
Chapter 1: Introduction to System IPCC Enterprise

Basic IPCC Call Flow
Chapter 2

IPCC Enterprise Platform Specifications

This section provides information on hardware and software specifications for IPCC Enterprise components. It also provides a list of any component features not supported when components are deployed as part of an System IPCC Enterprise deployment.

This section contains the following topics:

- About IPCC Enterprise Server Hardware Requirements, page 19
- About IPCC Enterprise Operating System Requirements, page 21
- About IPCC Enterprise Network and Active Directory Domain Requirements, page 21
- About IPCC Enterprise 3rd Party Software Requirements, page 22
- About IPCC Internationalization and Localization Support, page 22
- About IPCC Enterprise Component Version Interoperability, page 22
- Licensing Requirements and System Limitations, page 23
- About Non-Supported Component Features in an IPCC Environment, page 23

About IPCC Enterprise Server Hardware Requirements

IPCC 7.0(0) components are supported only on Cisco MCS or MCS-equivalent servers. See the Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials (BOM) for further specifics on hardware requirements including recommended platform sizing guidelines (not specific brands or models of servers), based on the types of available hardware systems. The BOM for IPCC Enterprise is available from cisco.com at: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_usage_guidelines_list.html.

The table below summarizes the box requirements for each IPCC component type. Refer to the Cisco IP Contact Center Enterprise Edition Solution Reference Network Design Guide for detailed deployment models, performance limitations, network considerations, and installation options.

Note: Always install the Controllers and Administration & WebView Reporting on a "clean" machine—that is, one which has a fresh install of the operating system and any prerequisite
software. Under no circumstances should the Controllers or Administration & WebView Reporting be installed on a domain controller or DNS server.

<table>
<thead>
<tr>
<th>IPCC Enterprise Component</th>
<th>Box Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CallManager</td>
<td>Must be installed on its own machine. Do not install other IPCC Enterprise components on the CallManager. System IPCC supports clustering of Call Managers.</td>
</tr>
<tr>
<td>IP IVR</td>
<td>Must be installed on its own machine. Do not install other IPCC Enterprise components on the IP IVR. System IPCC supports connections for up to five IP IVRs per Agent/IVR Controller. In deployments containing multiple IP IVRs, System IPCC’s Network VRU automatically balances load across the IP IVRs based on trunk availability.</td>
</tr>
<tr>
<td>Central Controller, Agent/IVR Controller, Administration &amp; WebView Reporting</td>
<td>All three can be installed on a single machine. Or the Central Controller and Agent/IVR Controller can be installed on the same machine and Administration &amp; WebView Reporting on another. Or all three can be deployed standalone. Do not install other IPCC Enterprise components on these machines. The Central Controller and Agent/IVR Controller can be duplexed for hardware fault tolerance. You can install two Administration &amp; WebView Reporting machines, although these machines are not duplexed.</td>
</tr>
<tr>
<td>Outbound Controller</td>
<td>Must be installed on its own machine. Do not install other IPCC Enterprise components on the Outbound Controller. The Outbound Controller cannot be duplexed.</td>
</tr>
<tr>
<td>Multichannel Controller</td>
<td>Multichannel Controllers for CCS and CEM must be installed on separate machines. You must install Media Blender on the Multichannel Controller for CCS. You must install the CEM T Server on the Multichannel Controller for CEM. Do not install any other IPCC Enterprise components on these machines. The Multichannel Controller cannot be duplexed.</td>
</tr>
<tr>
<td>Cisco Collaboration Server</td>
<td>The Cisco Collaboration Server (CCS) must be installed on its own machine. Do not install other IPCC Enterprise components on the Collaboration Server. Do not install the Cisco Collaboration Server on the same machine as Cisco Media Blender.</td>
</tr>
<tr>
<td>Cisco E-Mail Manager</td>
<td>The Cisco E-Mail Manager (CEM) T Server must be installed on the CEM Multichannel Controller. Do not install other CEM components on the Multichannel Controller. The E-Mail Manager database server and client must be installed on separate machines. Do not install other IPCC Enterprise components on other E-Mail Manager servers.</td>
</tr>
</tbody>
</table>
### IPCC Enterprise Component Requirements

<table>
<thead>
<tr>
<th>IPCC Enterprise Component</th>
<th>Box Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Media Blender</td>
<td>Must be installed on the same machine as the Multichannel Controller for CCS. Do not install any other IPCC Enterprise components on the Media Blender.</td>
</tr>
<tr>
<td>CTI OS or CAD</td>
<td>The CTI OS Server is installed automatically on the Agent/IVR Controller. CTI OS desktop software is installed on agent, supervisor, and CTI OS developer client machines. For smaller deployments, CAD Services can be deployed on the Agent/IVR Controller. For larger deployments, CAD Services can be installed on a separate machine. CAD desktop software is installed on agent, supervisor, and CAD developer client machines.</td>
</tr>
</tbody>
</table>

**About IPCC Enterprise Operating System Requirements**

See the following documents for operating system requirements for IPCC Enterprise components:

- For CallManager, see the CallManager Compatibility Matrix at [www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg)


- For all other IPCC Enterprise components, see the Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials at [http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm)

**About IPCC Enterprise Network and Active Directory Domain Requirements**

System IPCC 7.0(0) components require a Windows Active Directory domain. See the Staging Guide for ICM/IPCC Enterprise and Hosted Editions for further specifics on Active Directory configuration and other network configuration requirements. Additional network consideration and planning guidelines can be found into the Cisco IP Contact Center Enterprise Edition Solution Reference Network Design Guide

**Supported Windows Active Directory Models**

Under Windows, the IPCC software requires the use of Active Directory and DNS to maintain the Active Directory model. The account database that validates users in the domain is kept in the Active Directory. Windows has built-in methods to replicate this account database to the domain controllers within the forest and domain, across the various Active Directory sites.

See the Staging Guide for ICM/IPCC Enterprise and Hosted Editions for detailed information on supported Windows Active Directory models and requirements.
About IPCC Enterprise 3rd Party Software Requirements

Many IPCC components require certain prerequisite 3rd party software that must be loaded prior to installation. See the documents listed below to determine prerequisite software for each IPCC component.

See the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials* for information on supported 3rd party software version numbers.

<table>
<thead>
<tr>
<th>IPCC Component</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>CallManager</td>
<td><em>Installing Cisco CallManager</em></td>
</tr>
<tr>
<td>IP IVR</td>
<td><em>Cisco IP IVR Installation Guide</em></td>
</tr>
<tr>
<td>Central Controller, Agent/IVR Controller,</td>
<td>In the *Installing and Configuring the Controllers and Administration</td>
</tr>
<tr>
<td>Administration &amp; WebView Reporting, Multichannel</td>
<td>&amp; WebView Reporting (page 57) section of this guide</td>
</tr>
<tr>
<td>Controller, Outbound Controller</td>
<td></td>
</tr>
<tr>
<td>Cisco Collaboration Server</td>
<td>*Cisco Collaboration Server Installation Guide for Cisco ICM/IPCC</td>
</tr>
<tr>
<td></td>
<td>Enterprise &amp; Hosted Editions</td>
</tr>
<tr>
<td>Cisco Media Blender</td>
<td>*Cisco Media Blender Installation Guide for Cisco ICM/IPCC Enterprise</td>
</tr>
<tr>
<td></td>
<td>&amp; Hosted Editions</td>
</tr>
<tr>
<td>Cisco E-Mail Manager</td>
<td>*Cisco E-Mail Manager Installation and Configuration Guide for Cisco</td>
</tr>
<tr>
<td></td>
<td>ICM/IPCC Enterprise &amp; Hosted Editions</td>
</tr>
</tbody>
</table>

About IPCC Internationalization and Localization Support

See the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials* for information on System IPCC Enterprise Internationalization and Localization support.

About IPCC Enterprise Component Version Interoperability

See the *IPCC Compatibility Guide* for the list of Cisco IP Phone and IPCC component (e.g., CallManager, IP IVR, CTI OS) versions supported by IPCC Enterprise 7.0(0). The *IPCC Compatibility Guide* is updated regularly to reflect subsequent component releases and services releases.

The *IPCC Compatibility Guide* is available from cisco.com at:
Licensing Requirements and System Limitations

For licensing requirements and system limitations, see the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials.*

About Non-Supported Component Features in an IPCC Environment

Prior to installing and configuring IPCC Enterprise components, consult the *Release Notes for Cisco IPCC/ICM Enterprise & Hosted Editions Release 7.0(0)* for a list of any component features or configurations not supported in an IPCC Enterprise environment. Cisco CallManager in particular has certain features that cannot be used within IPCC Enterprise.

Chapter 2: - IPCC Enterprise Platform Specifications

About Non-Supported Component Features in an IPCC Environment
Chapter 3

System IPCC Deployment Models

This section contains the following topics:

• About System IPCC Deployment Models, page 25
• Choosing A Deployment Model: Load Considerations, page 28

About System IPCC Deployment Models

System IPCC Enterprise supports a number of different deployment models. The number of physical machines required for your System IPCC Enterprise deployment can vary depending on:

• Whether you choose to install the Central Controller, Agent/IVR Controller, and Administration & WebView Reporting on one machine (an All-in-One); two machines (a Central Controller-Agent/IVR Controller plus standalone Administration & WebView Reporting); or on three separate boxes.

Note: All-in-One deployments are supported in lab environments only.

• Whether you choose to deploy the Central Controller, Agent/IVR Controller, and Administration & WebView Reporting machine(s) as simplexed (one instance of each) or duplexed (two of each for enhanced fault tolerance).

• Whether you choose to deploy the multichannel and/or outbound options.

The following table and diagrams define individual box requirements and illustrate some sample System IPCC deployment model topologies.
### IPPC Enterprise Component

| IPPC Enterprise Component | Box Requirements | Can be Duplexed?
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CallManager</td>
<td>Must be installed on its own machine. Do not install other IPPC Enterprise components on the CallManager. Can be clustered.</td>
<td>No.</td>
</tr>
<tr>
<td>IP IVR</td>
<td>Must be installed on its own machine. Do not install other IPPC Enterprise components on the IP IVR. Note: System IPCC supports connections for up to five IP IVRs per Agent/IVR Controller. In deployments containing multiple IP IVRs, System IPCC's Network VRU automatically balances load across the IP IVRs based on trunk availability.</td>
<td>Yes</td>
</tr>
<tr>
<td>Central Controller</td>
<td>Can be installed standalone, or with an Agent/IVR Controller, or with an Agent/IVR Controller and Administration &amp; WebView Reporting. Do not install any other IPPC Enterprise components on this machine.</td>
<td>Yes</td>
</tr>
<tr>
<td>Agent/IVR Controller</td>
<td>Can be installed standalone, or with a Central Controller, or with a Central Controller and Administration &amp; WebView Reporting. Do not install any other IPPC Enterprise components on this machine.</td>
<td>No. However, two non-duplexed Administration &amp; WebView Reporting machines can be installed.</td>
</tr>
<tr>
<td>Administration &amp; WebView Reporting</td>
<td>Can be installed standalone, or with an with an Agent/IVR Controller and a Central Controller. Do not install any other IPPC Enterprise components on this machine.</td>
<td>No. However, two non-duplexed Administration &amp; WebView Reporting machines can be installed.</td>
</tr>
<tr>
<td>Outbound Controller</td>
<td>Must be installed on its own machine. Do not install other IPPC Enterprise components on the Outbound Controller.</td>
<td>No</td>
</tr>
<tr>
<td>Multichannel Controller</td>
<td>Multichannel Controllers for Cisco Collaboration Server (CCS) and Cisco E-Mail Manager (CEM) must be installed on separate machines. Install Media Blender on the Multichannel Controller for CCS. Install the CEM T Server on the Multichannel Controller for CEM. Do not install any other IPPC Enterprise components on these machines.</td>
<td>No</td>
</tr>
<tr>
<td>Cisco Collaboration Server</td>
<td>The Collaboration Server must be installed on its own machine. Do not install the Cisco Collaboration Server on the same machine.</td>
<td>No</td>
</tr>
<tr>
<td>IPCC Enterprise Component</td>
<td>Box Requirements</td>
<td>Can be Duplexed?</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>as Cisco Media Blender. Do not install other IPCC Enterprise components on the Collaboration Server.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>The E-Mail Manager database server and client must be installed on separate machines. Do not install other IPCC Enterprise components on the E-Mail Manager.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Must be installed on the same machine as the Multichannel Controller for CCS. Do not install any other IPCC Enterprise components on the Media Blender.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>The CTI OS Server is installed automatically on the Agent/IVR Controller. CTI OS desktop software is installed on agent, supervisor, and CTI OS developer client machines. For smaller deployments, CAD Services can be deployed on the Agent/IVR Controller. For larger deployments, CAD Services can be installed on a separate machine. CAD desktop software is installed on agent, supervisor, and CAD developer client machines.</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Choosing A Deployment Model: Load Considerations

In choosing a deployment model, consider the following guidelines and limitations:

- All-in-One deployments of the Central Controller, Agent/IVR Controller, and Administration & WebView Reporting are supported in lab environments only; Cisco does not support the use of All-in-Ones in a live, production environment.

- Light-load production environments may choose to deploy the Central Controller and Agent/IVR Controller on the same machine. Production environments that anticipate heavy call load should install the Central Controller and Agent/IVR Controller on separate machines for optimum performance.

- It is strongly recommended that all production environments use duplexed deployments of the Central Controller and Agent/IVR controller. Duplexed deployments add critical safeguards against machine failure.
Part 2: Installing and Configuring System IPCC Enterprise
Overview of Installation and Configuration Tasks

Setting up a System IPCC Enterprise system involves a significant number of installation and configuration tasks. This section includes task checklists designed to help you track your progress as you install and configure System IPCC.

This section contains the following topics:

- Hardware Installation Checklist, page 31
- IPCC Enterprise Staging Requirements, page 32
- IPCC Enterprise Component Software Installation Checklist, page 32
- IPCC Enterprise Component Software Configuration Tasks, page 34

Hardware Installation Checklist

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the Media Convergence Server(s) for Cisco CallManager, IP IVR, and IPCC.</td>
<td>Hardware and OS requirements for these servers are available from the Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials. Network architecture requirements are described in the Staging Guide for Cisco ICM/IPCC Enterprise &amp; Hosted Editions, and in the Cisco IP Contact Center Enterprise Edition Solution Reference Network Design Guide.</td>
</tr>
<tr>
<td>Install IP phones. Configure each IP phone with an IP address.</td>
<td>Install the IP phones after installing Cisco CallManager. If you are configuring the phones through auto-registration, also enable auto-registration on Cisco CallManager before installing the phones. Refer to the user documentation for your phone for information on IP address configuration requirements. Refer to the IPCC Enterprise Compatibility Guide for a list of supported IP Phones.</td>
</tr>
</tbody>
</table>
IPCC Enterprise Staging Requirements

Staging requirements include all network and OS platform prerequisite that must be in place before you install IPCC components. Staging requirements for IPCC components include:

- Windows OS configuration
- Windows network configuration
- Active Directory setup
- Firewall and security configuration
- SQLServer installation
- Remote monitoring and management tool setup (optional)
- Cisco Quality of Service (QoS) setup (optional)


IPCC Enterprise Component Software Installation Checklist

This section lists the installation tasks for the IPCC Enterprise software components.

Note: See the IPCC Enterprise Compatibility Guide for the list of Cisco IP Phone and IPCC component (e.g., CallManager, IP IVR) versions supported by IPCC Enterprise 7.0(0). The IPCC Compatibility Guide is updated regularly to reflect subsequent component releases and services releases. The IPCC Enterprise Compatibility Guide is available from cisco.com at:

<table>
<thead>
<tr>
<th>Task</th>
<th>IPCC Installation Prerequisites</th>
<th>IPCC Installation Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install CallManager</td>
<td>There are no IPCC-specific installation prerequisites for CallManager.</td>
<td>None</td>
</tr>
<tr>
<td>Task</td>
<td>IPCC Installation Prerequisites</td>
<td>IPCC Installation Notes</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------</td>
<td>-------------------------</td>
</tr>
</tbody>
</table>
| Install IP IVR | Prior to installing IP IVR you must install and configure Cisco CallManager. On the CallManager configuration, you must have:  
• Configured one CTI Route Point for each post route number and/or one for each translation route DNIS.  
• Configured CTI Ports for the IP IVR. The port numbers must match the port numbers used when installing the JTAPI interface on the IP IVR.  
• Created an IP IVR user and associated the user with CTI Route Point(s) and CTI Port(s).  
• Enabled CTI for the IP IVR user.  
**Note:** Note: In IP IVR version 4.0(x) and above IP IVR route points, CTI ports, and the JTAPI user for IP IVR can be created directly in the IP IVR administration interface; they do not need to be created in CallManager. | When installing IP IVR for use with IPCC Enterprise, be sure to select the ICM option during installation. This installs the basic IP IVR platform, which includes:  
• IP IVR profile in the DC Directory  
• Basic components of the IP IVR  
• Default IPCC scripts  
Installing IP IVR also installs the required JTAPI Client. You can use the JTAPI Client Update tool to ensure that you have the most recent version. |
| Install System IPCC Central Controller, Agent / IVR Controller, and Administration & WebView Reporting component. | Prior to installing the Central Controller, Agent / IVR Controller, and Administration & WebView Reporting component you must install and configure Cisco CallManager. On the CallManager, you must have:  
• Configured one CTI Route Point for each post route number and/or one for each translation route DNIS.  
• Created an Agent/IVR Controller user and associated the JTAPI user with CTI Route Point(s) and CTI Port(s).  
• Enabled CTI for the Agent/IVR Controller user.  
You must also install IP IVR. On the IP IVR, you must have:  
• Configured the VRU Port Group.  
• Configured the ICM subsystem.  
• Uploaded VRU scripts.  
• Specified the VRU Connection Port.  
• Configured translation routing on the IP IVR | None |
### IPCC Enterprise Component Software Configuration Tasks

Subsequent sections in this document guide you through configuring each IPCC component/functionality area. Each section contains a list of the configuration tasks for that component, as well as a list of prerequisites that must be met before that component can be configured.

1. Configure CallManager
2. Configure IP IVR
3. Configure the System IPCC Central Controller, Agent / IVR Controller, Administration & WebView Reporting component, Outbound Controller (if deployed), and Multichannel Controller(s) (if deployed).
4. Configure the Outbound Option feature (if deployed)
5. Configure Agent And Supervisor Desktops
6. Configure Multichannel applications (if deployed)
7. Configure reporting
Chapter 5

Installing and Configuring Cisco CallManager for System IPCC Enterprise

This section describes how to install and configure Cisco CallManager for System IPCC Enterprise.

Note: IPCC Enterprise 7.0(0) supports multiple CallManager versions. The instructions in the section are based on CallManager version 4.0(1).

This section contains the following topics:

- How to Install Cisco CallManager for IPCC Enterprise, page 35
- CallManager Configuration Tasks, page 36
- About the CallManager Administration Utility, page 36
- How to Configure Agent IP Phones for IPCC Enterprise, page 37
- About the CallManager Extension Mobility Feature, page 38
- How to Configure CTI Route Points, page 39
- How to Configure CTI Ports, page 40
- How to Configure JTAPI Users for the Agent/IVR Controller and IP IVR, page 41

How to Install Cisco CallManager for IPCC Enterprise

To install Cisco CallManager, follow the step-by-step installation instructions included in the Installing Cisco CallManager Guide. There are no IPCC-specific installation prerequisites or instructions for CallManager.
Once installation is complete, confirm that the following are true before you begin configuring CallManager for IPCC Enterprise:

- A CallManager instance has been created on the CallManager server.
- All CallManager services and third-party services required by CallManager are running.
- The BAT Tool has been installed on the CallManager.

See Also

* Installing Cisco CallManager Guide
* Bulk Administration Tool Guide for Cisco CallManager

## CallManager Configuration Tasks

After you install CallManager, complete these tasks to configure CallManager for use with IPCC. Perform tasks in the order listed. Instructions for each are included later in this section.

<table>
<thead>
<tr>
<th>CallManager Configuration Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure the agent IP phones.</td>
<td>Prior to this, you must have installed your Cisco IP phones on your network. For instructions, refer to the documentation packaged with your Cisco IP phone.</td>
</tr>
<tr>
<td>2. Configure the CTI Route Points.</td>
<td>Note: If you are using IP IVR 4.0(x) or later, the CTI Route Points controlled by the IP IVR can be configured directly in the IP IVR Administration interface; you do not need to configure them in CallManager. The Route Points for dialed numbers must still be created in CallManager Administration.</td>
</tr>
<tr>
<td>3. Configure the CTI Ports.</td>
<td>Note: If you are using IP IVR 4.0(x) or later, CTI Ports can be configured directly in the IP IVR Administration interface; you do not need to configure them in CallManager.</td>
</tr>
<tr>
<td>4. Create JTAPI user accounts and associate them with the JTAPI phones, Route Points, and Ports.</td>
<td>Create one account to associate with the phones and Agent/IVR Controller, and one account to associate with IP IVR and the CTI Ports. Note: If you are using IP IVR 4.0(x) or later, the JTAPI user for the IP IVR can be created directly in the IP IVR Administration interface.</td>
</tr>
</tbody>
</table>

## About the CallManager Administration Utility

Most of the tasks in this section are performed from the CallManager Administration utility. CallManager Administration is installed on all CallManager servers. To access CallManager Administration, select Start > Programs > Cisco CallManager > Administration. Or, in a Web browser, enter http://<CallManager_servername>/ccmadmin.
How to Configure Agent IP Phones for IPCC Enterprise

How to Configure IP Phones on the CallManager

To function with CallManager, each Cisco IP phone in your IPCC Enterprise system must be registered and configured within the CallManager Administration database.

There are three different ways of doing this:

• Manual configuration: In manual configuration, each agent IP phone is configured individually. This is the configuration method described in this document.

• Auto-registration: Auto-registration allows you to automatically add a Cisco IP Phone to the Cisco CallManager database when you connect the phone to your IP telephony network. During auto-registration, Cisco CallManager assigns the next available sequential directory number to the phone. In many cases, you might not want to use auto-registration; for example, if you want to assign a specific directory number to a phone. The procedure for setting up auto-registration is not described in this guide. For instructions, see the Cisco CallManager Administration Guide.

• Bulk configuration: The CallManager Bulk Administration Tool is a plug-in application that lets you add, modify, and delete multiple Cisco IP Phones in batch mode. Procedures for using the Bulk Administration Tool are not described in this guide. For instructions, see the Bulk Administration Tool Guide for Cisco CallManager.

To manually configure agent IP phones on the CallManager, perform the following steps for each agent IP Phone in your IPCC Enterprise System:

**Step 1** In CallManager Administration, select Device > Add a Device.

**Step 2** From Device Type, select Phone. Click Next.

**Step 3** From Phone Type, select the model of Cisco IP phone you are configuring. Click Next.

**Step 4** In the MAC Address field, enter the phone's MAC address. To determine an IP phone's MAC address consult the sticker on the back of the phone, or, on the phone, select Settings > Network Configuration > Select.

**Step 5** From Device Pool, select Default.

**Step 6** Click Insert. A message displays asking if you want to add a directory number for line 1 of this phone now. Click OK.

**Step 7** In Directory Number, enter the directory number for this phone. This will be the agent's ID for logging into the phone.

**Step 8** Set the Call Waiting field. If the agent using this phone:
Will use IPCC’s Outbound Option feature (which allows outbound calling), set Call Waiting to On.

Will not use Outbound Option set Call Waiting to Off. Disabling Call Waiting ensures that the forward on busy option is available.

Note:

- If no agents on this CallManager will make outbound calls, you can set the CallManager system default for Call Waiting Enable to Off. See the CallManager Administration online Help for instructions on setting CallManager system defaults.
- The Call Waiting option does not appear and is on by default in CallManager versions 4.0(1) and greater.

Step 9  Click Insert. A message displays confirming the device record has been created in the CallManager database. Click OK.

Step 10 Create additional phones, as necessary.

How to Set the Agent IP Phone Configuration on the IP Phone

You must set the configuration on each agent IP phone so that it can locate and connect to Cisco CallManager. To set the necessary configuration, on each agent IP phone in your IPCC Enterprise system:

Step 1  Press Settings.

Step 2  Press **# to unlock the configuration.

Step 3  Select Settings > Network Configuration > Select.

Step 4  Set Alternative TFTP to Yes.

Step 5  Press Save and then press Exit.

Step 6  Power cycle the phone. If you are using power plugs, pull the cord out of the phone and put it back in again. If you are using inline power, disconnect and then reconnect the network cable.

About the CallManager Extension Mobility Feature

CallManager provides an Extension Mobility feature that lets users access their Cisco IP phone configuration, including line appearances, services, and speed dials, from other Cisco IP phones. If you enable Extension Mobility, agents can share the same IP phone and retain their personal settings. In an IPCC Enterprise system, IP phones with Extension Mobility have the same behavior and features as regular IP phones. Procedures for enabling Extension Mobility are not described in this guide. For instructions, see the Cisco CallManager Features and Service Guide.
How to Configure CTI Route Points

A CTI Route Point is a virtual device that can receive multiple concurrent calls for application-controlled redirection. Calls are directed to a route point, which subsequently routes the call to an available CTI port—the front end of the redirection application. The CTI route point is the number a caller dials to access the application. At least one CTI route point must be configured for each redirection application in use. In IPCC Enterprise, these applications include IP IVR and Cisco JTAPI running on the Agent/IVR Controller.

Once a CTI route point has been created, lines (directory numbers) can be added and configured. CTI route points are used for post-routing with IPCC. In the event that the Agent/IVR Controller is down or the IPCC cannot route a call, you can post-route the call to another CTI Route Point.

Note: If you are using IP IVR 4.0(x) or later, the CTI Route Points controlled by the IP IVR can be configured directly in the IP IVR Administration interface; you do not need to configure them in Call Manager. Consult your IP IVR documentation for instructions. The Route Points for dialed numbers must still be created in CallManager Administration.

To configure a CTI Route Point:

**Step 1**
In CallManager Administration, select Device > Add New Device.

**Step 2**
From Device Type, select CTI Route Point. Click Next.

**Step 3**
In Device Name, enter the Route Point name.

**Step 4**
From Device Pool, select Default.

**Step 5**
Click Insert. A message displays confirming the device record has been created in the CallManager database. Click OK.

**Step 6**
In Directory Number, enter the number of this device.

Note: Record the directory number that you enter; You will need it later when you A) configure a port group for translation routing in IP IVR and B) configure the Network IVR in the IPCC Web Administration Tool.

**Step 7**
From Call Waiting, select On.

Note: The Call Waiting option does not appear and is on by default in CallManager versions 4.0(1) and greater.

**Step 8**
Optionally, in Forward All, Forward Busy, Forward No Answer, and Forward on Failure, enter the directory numbers of the device that you want the call to go to in the event that IPCC cannot route the call.

**Step 9**
Click Insert.
How to Configure CTI Ports

A CTI Port is a virtual port analogous to a trunk line in a traditional ACD or PBX setting. The CTI Port allows access to the post-routing capabilities of IP IVR.

The number of ports you configure is determined by your needs and available licenses. In order to accept or place calls, the JTAPI subsystem requires one CTI port device for each call to be managed simultaneously.

If you are using IP IVR 4.0(x) or later, CTI Ports can be configured directly in the IP IVR Administration interface; you do not need to configure them in Call Manager. Consult your IP IVR documentation for instructions.

Note: If you are using IP IVR 4.0(x) or later, CTI Ports can be configured directly in the IP IVR Administration interface; you do not need to configure them in Call Manager. Consult your IP IVR documentation for instructions.

To configure CTI ports:

1. In CallManager Administration, select Device > Phone.
2. Click Add a New Phone.
3. From Phone Type, select CTI Port. Click Next.
4. In Device Name, enter a unique name for the device.
5. From Device Pool, select Default.
6. Click Insert. A message displays confirming the device record has been created in the CallManager database. Click OK.
7. In Directory Number, enter a dialable phone number. Values can include numeric characters and route pattern wildcards and special characters except for (.) and (@).
8. From Call Waiting, select Off.
   **Note:** The Call Waiting option does not appear and is on by default in CallManager versions 4.0(1) and greater.
9. Click Insert. A message displays confirming the directory number has been assigned to the current device. Click OK.
10. Repeat these steps to create additional port groups, as necessary.
How to Configure JTAPI Users for the Agent/IVR Controller and IP IVR

Cisco CallManager supports the Java Telephony Application Programming Interface (JTAPI) for deploying telephony applications. JTAPI gives IPCC access to the Cisco CallManager directory. JTAPI uses the directory to determine which IPCC devices it has the privilege to control.

A user account must be associated with each JTAPI device. For IPCC Enterprise, you must create a JTAPI user for 1) the connection to the IPCC Agent/IVR Controller, and 2) the connection to each IP IVR in your deployment.

**Note:** If you are using IP IVR 4.0(x) or later, the JTAPI user for IP IVR can be configured directly in the IP IVR Administration interface; you do not need to configure them in Call Manager. You must still create the JTAPI user for the CallManager PG in CallManager Administration.

To configure JTAPI users for the Agent/IVR Controller and IP IVR:

1. **Step 1** In CallManager Administration, select User > Add a New User. The User Information page opens.
2. **Step 2** Enter a first and last name for the user.
3. **Step 3** In UserID, enter the User ID for the Agent/IVR Controller user.
4. **Step 4** In User Password, enter a password. Re-enter it in Confirm Password.
5. **Step 5** In PIN, enter an IP phone password (at least five characters). Re-enter it in Confirm PIN.

   **Note:** Record the user names and passwords that you create for the JTAPI users. You will need to supply these when you configure A) CallManager connectivity for the Agent/IVR Controller in IPCC Web Administration; B) the IP IVR JTAPI user in CRA Admin.

6. **Step 6** Select Enable CTI Application Use.
7. **Step 7** Click Insert.
8. **Step 8** Under Application Profiles, click Device Association.
9. **Step 9** Click Select Devices. All the Device names and extensions display. Select all of the devices this user will control.
   - For the Agent/IVR Controller user, select the IP phones and the Agent/IVR Controller route points.
   - For the IP IVR user, select the IP IVR route points and the ports.
10. **Step 10** Select No Primary Extension.
11. **Step 11** Click Update.
About the CallManager Extension Mobility Feature

Step 12  Repeat these steps to create additional JTAPI users as necessary.

See Also

Installing Cisco CallManager Guide
Cisco CallManager Administration Guide
Bulk Administration Tool Guide for Cisco CallManager
Cisco CallManager Features and Service Guide
Installing and Configuring Cisco IP IVR for IPCC Enterprise

This section describes how to install and configure Cisco IP IVR for System IPCC Enterprise.

**Note:**

- IPCC Enterprise 7.0(0) supports multiple IP IVR versions. The instructions in the section are based on IP IVR version 3.5(x). Subsequent versions of IP IVR offer enhanced capabilities for automatically synchronizing settings in IP IVR with CallManager, including the ability to create route points, port groups, and JTAPI users directly within the IP IVR administration interface. For more information, see your IP IVR documentation.

- Based on your licensing, the IP IVR version you are running may be named “IP IVR” or “IP Queue Manager.” In either case, the instructions for deploying it with IPCC are the same. “IP IVR” is the term used throughout this guide.

This section contains the following topics:

- About IP IVR, page 44
- About IP IVR Installation Prerequisites, page 44
- How to Install IP IVR for IPCC Enterprise, page 44
- IP IVR Configuration Tasks, page 45
- About the CRS Administration Utility, page 46
- How to Configure the Directory Profile, page 46
- How to Configure the JTAPI User on the IP IVR System, page 48
- How to Configure CTI Port Groups, page 48
- How to Configure the ICM Subsystem, page 50
- How to Configure and Upload VRU Scripts, page 50
- About Translation Routing and Post Routing, page 51
- How to Configure IP IVR for Translation Routing, page 52
- How to Configure IP IVR for IPCC Post Routing, page 54
- How to Configure and Start the Application Engine, page 55
- How to Verify and Update the JTAPI Client, page 55
About IP IVR

Cisco IP IVR provides Interactive Voice Response (IVR) and queuing capability in the IPCC system. Cisco IP IVR is a multichannel (voice/data/Web) IP-enabled Interactive Voice Response solution that provides an open, extensible, and feature-rich foundation for the creation and delivery of IVR solutions using Internet technology. In addition to handling traditional telephony contacts, you can create IP IVR applications to respond to HTTP requests and send e-mail messages.

Note: IPCC Enterprise does not support CRS clustering (duplexed IP IVRs that failover to the same CTI route points). Additionally, CRS (IP IVR) 4.0(x) does not allow multiple clusters to share the repository profile for scripts.

About IP IVR Installation Prerequisites

Before installing and configuring IP IVR for use with IPCC Enterprise, you must:

<table>
<thead>
<tr>
<th>IP IVR Installation Prerequisite</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Install and configure Cisco CallManager | On the CallManager configuration, you must have:  
  • Configured your IP phones.  
  • Configured one CTI Route Point for each post route number and/or one for each translation route DNIS.  
  • Configured CTI Ports for the IP IVR. The port numbers you use when installing the JTAPI interface on the IP IVR must match these numbers.  
  • Created an IP IVR user and associated the user with CTI Route Point(s) and CTI Port(s). Enabled CTI for the IP IVR user. |

Note: In IP IVR versions 4.0(x) and above these prerequisite items can be created directly in the IP IVR administration interface. They do not need to be created in CallManager. For more information, see your IP IVR documentation.

How to Install IP IVR for IPCC Enterprise

To install Cisco IP IVR, follow the step-by-step installation instructions included in the Cisco Customer Response Applications Installation Guide.
When installing IP IVR for use with IPCC Enterprise, you must select the ICM option during installation. This installs the basic IP IVR platform, which includes:

- IP IVR profile in the DC Directory
- Basic components of the IP IVR
- Default IPCC scripts

Installing the IP IVR also installs the required JTAPI Client. (As necessary, you can use the JTAPI Client Update Tool to ensure that you have the most recent version. See How to Verify and Update the JTAPI Client for instructions.)

Once installation is complete, confirm that the following are true before you begin configuring IP IVR for IPCC Enterprise:

- In the CRS Administration utility, ICM appears under the subsystems menu. If it does not, a modification to the license (.lic) file may be required.

### IP IVR Configuration Tasks

After you install IP IVR, complete these tasks to configure IP IVR for use with IPCC Enterprise Environment. Perform tasks in the order listed. Instructions for each are included later in this section.

<table>
<thead>
<tr>
<th>IP IVR Configuration Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure the Directory Profile.</td>
<td>Make note of the host name.</td>
</tr>
<tr>
<td>2. Configure JTAPI user on IP IVR.</td>
<td></td>
</tr>
<tr>
<td>3. Configure CTI Port Groups.</td>
<td></td>
</tr>
<tr>
<td>4. Configure the ICM Subsystem.</td>
<td></td>
</tr>
<tr>
<td>5. Create and upload VRU scripts.</td>
<td></td>
</tr>
<tr>
<td>7. Configure and start the Application Engine.</td>
<td></td>
</tr>
</tbody>
</table>
About the CRS Administration Utility

Most of the tasks in this section are performed from the Customer Response Applications Administration utility. CRS Administration is installed on your IP IVR server. Access the CRS Administrator at: http://<ipivr_server name>/appadmin.

How to Configure the Directory Profile

You must create a directory profile for each Cisco IP IVR system. The directory profile contains the directory host name or IP address, directory port number, directory user (DN), directory password, base context, server type, and the configuration profile name. There are two directories associated with each IP IVR system: the Configuration Directory and the Repository.

Each IP IVR system has its own Configuration Directory in the Lightweight Directory Access Protocol (LDAP) directory for storing configuration information.

The Repository is the subdirectory of the LDAP directory where the IP IVR scripts are stored. By default, every time you create a configuration directory, the Cisco Application Administration creates an identically named repository, but if you select the check box for the use a different repository profile option, multiple IP IVR directory profiles can share one easily updated repository. The repository keeps one backup version of each script for recovery purposes. You can revert to the previous version if necessary. You manage IP IVR scripts with the Repository Manager, which is installed with both the Cisco Application Editor and the Cisco Application Engine.

To configure the Directory Profile:

**Step 1**
In CRS Administration, select System > Configuration and Repository.

**Step 2**
From Server Type, select DC Directory.

**Step 3**
In Directory Host Name, enter the host name or IP address of the Cisco IP Telephony Directory server where the configuration profile resides or will reside with the CRS Engine profile. This information must be consistent with that entered in the CTI Manager A area on the CTI Manager Locations pane during CRS installation.

Optionally, enter the host names or IP addresses of alternative directory servers to be used in the event of a failover. Enter these in the order they should be used if failover occurs. Use semicolons, commas, or spaces to separate multiple entries. The information entered in this field must be consistent with the information entered in the CTI Manager B area on the CTI Manager Locations pane during CRS installation.

**Step 4**
In the Directory Port Number field, enter the port number of the Cisco IP telephony directory. The default is 8480.

**Step 5**
In the Directory User (DN) field, enter the username (called the distinguished name) configured on the directory server for the user with permission to modify the Cisco IP Telephony tree and object entries, or accept the default information.
Step 6  In the Directory Password field, enter a password for the directory user.

Step 7  In the Base Context field, enter the branch of the Cisco IP Telephony Directory tree that contains the Cisco configuration information, or accept the default information.

Step 8  In the User Base field, enter the branch of the Cisco IP Telephony Directory tree that contains user information, or accept the default information.

Step 9  Click Next.

Step 10 In the Profile Name field, perform one of the following tasks:

- From the drop-down list, choose the profile name that identifies this server configuration or repository. Or...

- Click Edit.

Step 11 Enter a new profile name. Click OK.

Step 12 Click Next.

Step 13 Perform one of the following tasks:

- To create the repository profile on the same server as your configuration profile, accept the default setting.

- To maintain separate profiles for your configuration and repository, click the Use a Different Repository Profile radio button. The Repository Configuration dialog box opens. Complete the fields with configuration information appropriate for your repository directory, and then click OK.

Step 14 Click Next. The User Maintenance page opens. If you want to find a specific Cisco CallManager user, enter search criteria (such as a user name) in the Enter Search Criteria text field and click Search. If more than 75 users are configured on Cisco CallManager, you can search for users who are not displayed.

Step 15 From the CMUsers list box, select one or more Cisco CallManager users, and then click < to move the selected users to the CRS Administrator/Supervisor list box

Step 16 For each user moved to the CRS Administrator/Supervisor list box, select a user in the list box and choose either Administrator or Supervisor from the Group drop-down list. Because only an administrator can update the CRS system, you must select at least one user to become an administrator.

Step 17 Click Finish to complete the process and initialize configuration and repository profiles. The Directory Setup page displays your configuration choices.

You are now ready to use the Application Administration web interface to administer your IP IVR system.
How to Configure the JTAPI User on the IP IVR System

When configuring CallManager, you configured a JTAPI user for your IP IVR. This user must now be identified in the IP IVR software.

**Note:** In IP IVR version 4.0(x) and above, you do not need to create the IP IVR JTAPI user in the CallManager Administration. Instead, follow the steps below and the user will be automatically created on the CallManager.

To configure the JTAPI user for IP IVR:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In CRS Administration, select Subsystems &gt; JTAPI.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the JTAPI provider(s) field, enter your CallManager's host name or IP address.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the UserID and password fields, enter the information that you created in Cisco CallManager for the IP IVR user.</td>
</tr>
</tbody>
</table>

**Note:** In IP IVR version 4.0(x) and above, rather than UserID you enter a User Prefix. IP IVR JTAPI users will then be automatically created on the CallManager with the ID <prefix>_<IP IVR node #>—for example, IPIVR_JTAPI_1.

| Step 4 | Click Update. |

How to Configure CTI Port Groups

A CTI Port Group is a group of access points into the IPCC telephone network. You use CTI Port Groups to associate Cisco IP IVR applications, translation routes, post routes, bust treatments, and reroute on ring no answer treatments with an IPCC trunk group.

A CTI port is a virtual device that is used by Cisco CallManager applications, including IP IVR, to create virtual lines. CTI ports are configured through Cisco CallManager Administration. CTI ports in a CTI Port Group must have consecutive directory numbers. For example, if you want twenty CTI ports in a particular CTI port group, and the first number is 9001, the rest of the ports will be 9002 through 9020. With twenty ports, the IP IVR can handle twenty calls at a time.

**Note:**

- If your system is co-located with Cisco CallManager, you can configure a maximum of 256 CTI ports in total for all CTI port groups. Configuring more CTI ports than this limit results in calls being aborted by the system in an unspecified manner.

- In IP IVR versions 4.0(x) the procedure for creating and configuring port groups varies from those listed below. In IP IVR 4.0(x), CRA Admin prompts you for CTI Port information and automatically creates the necessary records on the CallManager. For more information, see your IP IVR documentation.
If you are deploying IPCC with multiple IP IVRs, each CTI Port Group must have a unique Group ID across all IP IVRs configured in system. System IPCC requires the use of specific port group IDs for post and translation routing (see steps below).

To configure a CTI port group:

**Step 1** In CRS Administration, select Subsystems > JTAPI. (Note: System > Control Center in IP IVR 4.0(x)).

**Step 2** Click CTI Port Groups.

**Step 3** Click Add a New JTAPI Call Control Group.

**Step 4** In Group ID field, enter a unique ID for the port group. In System IPCC, you MUST use the following port group IDs:

- For IP IVR 1 (the first physical IP IVR in your deployment), Post Route Port Group ID = 0, Translation Route Port Group ID = 1
- For IP IVR 2, Post Route Port Group ID = 2, Translation Route Port Group ID = 3
- For IP IVR 3, Post Route Port Group ID = 4, Translation Route Port Group ID = 5
- For IP IVR 4, Post Route Port Group ID = 6, Translation Route Port Group ID = 7
- For IP IVR 5, Post Route Port Group ID = 8, Translation Route Port Group ID = 9

**Step 5** Press the Tab key to automatically populate the Description field.

**Step 6** From Calling Search Space for Redirect, select the option that specifies the search space, or partition, that the calling device searches when attempting to redirect the call.

**Step 7** Click Associate CTI Ports.

**Step 8** From the Available CTI Port List Filters drop-down lists, choose Device Name and Is Exactly, and then click the Find button.

The Directory Number and Device Name of the CTI port appear under their respective columns.

**Step 9** Select the CTI ports you want to associate with this port group.

**Step 10** Click Update.

**Step 11** Click Add.

**Step 12** As necessary, repeat these steps to create additional port groups and associate them with CTI ports.
How to Configure the ICM Subsystem

The ICM Subsystem on IP IVR allows IP IVR to interact with IPCC. It is the queuing engine for IPCC Enterprise. The IPCC Service Control interface allows IPCC to provide call processing instructions to IP IVR. It also provides IPCC with event reports indicating changes in call state.

To configure the ICM Subsystem:

**Step 1**
In CRS Administration, select Subsystems > ICM.

**Step 2**
In the VRU Connection Port field, enter the TCP IP port number on the IP IVR machine that the IPCC Agent/IVR Controller will use to communicate to IP IVR. The default value is 5000. Use the default unless you have a compelling reason to use a different port.

*Note:* Record the VRU Connection Port that you enter. You need to configure IVR connectivity in the IPCC Web Administration Tool with this number.

**Step 3**
In the Service Control field, click the Yes radio button. The Service Control interface allows the Agent/IVR Controller to provide call-processing instructions to IP IVR. It also provides IP IVR with event reports indicating changes in call state. You must enable the service control interface to use the ICM Subsystem.

**Step 4**
In the Parameter Separator field, enter the character used to delineate individual parameters in a multiple parameter variable or accept the default ( | (pipe)).

**Step 5**
In the Additional VRU Call Information check boxes, check any expanded call variables you want to use to pass call-related information.

**Step 6**
Click Update. The configuration information is added to the system.

How to Configure and Upload VRU Scripts

IPCC Enterprise uses Voice Response Unit (VRU) scripts to handle interactions with contacts. These scripts are loaded as applications on the CRS Engine.

IP IVR comes with some default scripts that are loaded as applications on the CRS Engine. You also can create your own VRU scripts using the Cisco CRS Editor. When configuring IPCC, you configure any VRU scripts that you plan to use. You must upload the scripts to the IP IVR Repository so the scripts will be available if IPCC sends a Run VRU Scripts request to IP IVR.

*Note:* Note: The CRS administration interface uses the term "VRU." The IPCC Web Administration Tool interface uses the term "IVR." These mean the same thing. Therefore, "VRU scripts" = "IVR scripts."

To configure VRU Scripts:

**Step 1**
In CRS Administration, select Subsystems > ICM.
Step 2  Click ICM VRU Scripts.

Step 3  Click Add a New VRU Script.

Step 4  In the VRU Script Name field, enter a name for the VRU script you want to add.

Step 5  In the Script field:

• From the Script drop-down list, choose the CRS script that you want to associate with the VRU script. OR...

• Click the Edit button. The User Prompt dialog box opens. Enter the name of the script, and then click OK. The User Prompt dialog box closes, and the name you entered appears in the Script field.

Note: Record the name of the script you enter. You need to configure IVR scripts in IPCC Web Administration with this value.

Step 6  Click Add.

The second ICM VRU Script area closes, and the name of the VRU script you added appears in the first ICM VRU Scripts area.

Step 7  Repeat these steps to add any additional VRU scripts.

About Translation Routing and Post Routing

Depending on how you choose to do call routing, you must configure your IPCC deployment for post routing and possibly translation routing as well.

Translation Routing

In translation routing, IPCC receives the call instead of IP IVR. Since IP IVR does not receive the call first, it does not run an initial script. After receiving the call, IPCC runs a script. You must configure Cisco IPCC translation routing when IP IVR is used as a queue point for a Cisco IPCC solution in which calls are expected to be routed by the Agent/IVR Controller to IP IVR. The call attributes will be reported as part of a configured translation-route on IPCC.
IPCC routing scripts can direct calls based on various criteria, such as time of day or the availability of subsystems. IPCC routing scripts can use four commands to interact with IP IVR:

- **Connect** connects the call. IPCC sends the connect message with a label to instruct IP IVR where to direct the call.
- **Release** hangs up the call.
- **Run VRU Script** runs a VRU script on IP IVR.
- **Cancel** cancels the VRU script that is currently running.

**Post Routing**

In post routing, IP IVR receives calls directly from CallManager. CallManager sends the call to the post routing route point on IP IVR. IP IVR searches the designated port group for a free CTI port and accepts the call. If there is not a free port, the caller hears ringing until there is a free port to take the call.

If you configured the route point to run an initial application, such as a script to welcome the caller and collect an account number, IP IVR runs that script, notifies IPCC about the call, and waits for further instructions. If you did not configure an initial application, IP IVR just informs IPCC. IPCC runs a routing script after being notified of the call. The IP IVR system responds to the commands from IPCC until it signals that the call is complete.

For example, the IPCC routing script could send a Run VRU Script request to IP IVR, instructing IP IVR to run a VRU script that plays music and thanks the caller for their patience. When an agent becomes available, IPCC sends a Cancel request and IP IVR stops running the current VRU script. IPCC then sends a Connect command with a Normal label that indicates the extension of the free agent. The IP IVR system routes the call to the agent indicated on the label.

**Note:** System IPCC does not support post routing within System IPCC deployment. However, post routing is supported between a child System IPCC and its parent in an IPCC Gateway deployment. (See your IPCC Gateway documentation for more information.)

**How to Configure IP IVR for Translation Routing**

To configure IP IVR for translation routing, you first add an ICM translation routing application and then assign a JTAPI trigger to this application.

**Note:** Before you can configure a translation routing application, you must first upload any VRU scripts that the application will need.

To configure IP IVR for translation routing:

**Step 1** In CRS Administration, select Applications > Configure Applications.

**Step 2** Click Add a New Application.

**Step 3** From Application Type, select Cisco ICM Translation-Routing.
Step 4 In the Name field, enter the name of the script on which the IPCC translation-routing is based.

Step 5 Press the Tab key to automatically populate the Description field.

Step 6 In the ID field, accept the ID, or enter a unique ID. This field corresponds to the service identifier of the call reported to the Cisco ICM and configured in the Cisco ICM translation route.

Step 7 In Maximum Number of Sessions, enter the maximum number of sessions that the application will be able to handle simultaneously.

Step 8 In the Enabled field, accept the default radio button Yes.

Step 9 In the Timeout (in secs) field, enter a value (in seconds). This value is the maximum amount of time the system will wait to invoke the application before rejecting a contact.

Step 10 From the Default Script drop-down list, choose the script that will be run if a system error occurs, or if instructed by the Cisco ICM to route to the default treatment.

Step 11 Click Add. A message displays confirming the operation has been successfully executed.

Step 12 Click OK.

Step 13 Click Add New Trigger. The Add a New JTAPI Trigger page opens.

Step 14 From Trigger Type, select , and then click Next.

Step 15 From CTI Route Point Directory Number, choose the CTI route point number that you configured for translation routing in the Cisco CallManager.

Step 16 From the Language drop-down list, choose the appropriate language, or accept the default language. The Application Name field is automatically populated with the Application Name.

Step 17 In Maximum Number of Sessions, enter the maximum number of sessions that can be simultaneously triggered by this trigger; for translation routing, this number is the same as the number of ports available for translation routing.

Step 18 In Idle Time-out (in ms), enter a maximum value (in milliseconds). This value is the maximum amount of time that the system will wait before rejecting a call.

Step 19 In the Enabled field, accept the default radio button Yes.

Step 20 From the Call Control Group drop-down list, choose the appropriate call control group.

Step 21 From the Primary Dialog Group drop-down list, choose the appropriate primary dialog group, or none.

Step 22 From the Secondary Dialog Group drop-down list, choose the appropriate secondary dialog group, or none.

Step 23 Click Add.
How to Configure IP IVR for IPCC Post Routing

To configure IP IVR for post routing, you first add an ICM post routing application and then assign a JTAPI trigger to this application.

**Note:** Before you can configure an IPCC routing application, you must first upload any VRU scripts that the application will need.

To configure IP IVR for post routing:

**Step 1** In CRS Administration, select Applications > Configure Applications.

**Step 2** Click Add a New Application.

**Step 3** From Application Type, select Cisco ICM Post-Routing.

**Step 4** In the Name field, enter the name of the script on which the translation-routing is based.

**Step 5** Press the Tab key to automatically populate the Description field.

**Step 6** In the ID field, accept the ID, or enter a unique ID. This field corresponds to the service identifier of the call reported to the Cisco ICM and configured in the Cisco ICM translation route.

**Step 7** In Maximum Number of Sessions, enter the maximum number of sessions that the application will be able to handle simultaneously.

**Step 8** In the Enabled field, accept the default radio button Yes.

**Step 9** In the Timeout (in secs) field, enter a value (in seconds). This value is the maximum amount of time the system will wait to invoke the application before rejecting a contact.

**Step 10** From the Default Script drop-down list, choose the script that will be run if a system error occurs, or if instructed by IPCC to route to the default treatment.

**Step 11** Click Add. A message displays confirming the operation has been successfully executed.

**Step 12** Click OK.

**Step 13** Click Add New Trigger.

The Add a New Trigger page opens.

**Step 14** From Trigger Type, select JTAPI, and then click Next.

**Step 15** From CTI Route Point Directory Number, choose the CTI route point number that you configured for post routing in the Cisco CallManager.

**Note:** Record this value. You will need it when you configure the Network IVR in IPCC Web Administration.
Step 16  From the Language drop-down list, choose the appropriate language, or accept the default language. The Application Name field is automatically populated with the Application Name.

Step 17  In Maximum Number of Sessions, enter the maximum number of sessions that can be simultaneously triggered by this trigger; for translation routing, this number is the same as the number of ports available for translation routing.

Step 18  In Idle Time-out (in ms), enter a maximum value (in milliseconds). This value is the maximum amount of time that the system will wait before rejecting a call.

Step 19  In the Enabled field, accept the default radio button Yes.

Step 20  From the Call Control Group drop-down list, choose the appropriate call control group.

Step 21  From the Primary Dialog Group drop-down list, choose the appropriate primary dialog group, or none.

Step 22  From the Secondary Dialog Group drop-down list, choose the appropriate secondary dialog group, or none.

Step 23  Click Add.

---

### How to Configure and Start the Application Engine

The Application Engine is a group of Java beans that can be combined in many ways to create applications such as IP IVR. The Application Engine is the execution vehicle for IP IVR flows, or scripts.

The subsystems will not start until the configuration of all elements is complete and valid. After completing all of the IPCC configuration, return to this topic to configure and start the Application Engine.

To configure and start the Application Engine:

**Step 1**  In CRS Administration, select System > Engine. (Note: System > Control Center in IP IVR 4.0(x))

**Step 2**  Configure the engine parameters as needed. You can also monitor engine activity from this page. Consult the CRA Administration online Help for more information.

**Step 3**  Click Start Engine.

---

### How to Verify and Update the JTAPI Client

During installation, the IP IVR installer automatically detects the JTAPI Client used by the specified CallManager server and installs this JTAPI Client on the server.
If you change versions of Cisco CallManager after installing IP IVR, CallManager may use a different version of the JTAPI Client than the version used by IP IVR. The JTAPI Client Update Tool enables you to update the JTAPI Client on the CRS server and Cisco Agent Desktop to the same JTAPI Client version used by Cisco CallManager.

The JTAPI Client Update Tool is installed by default in the C:\Program Files\wfavvid directory and is accessible from the Windows Start menu under Programs > Cisco CRS Administration.

See Also

Cisco Customer Response Applications Installation Guide

Cisco Customer Response Application Administration Guide
Chapter 7

Installing and Configuring the Controllers and Administration & WebView Reporting

This section describes how to install and configure the Central Controller, Agent/IVR Controller, Administration & WebView Reporting, and Multichannel and Outbound Controllers for IPCC Enterprise.

This section contains the following topics:

- 3rd Party Software: Prerequisite Installations, page 57
- 3rd Party Software: Packaged Software, page 58
- Installation Guidelines, page 59
- Installing and Configuring the Controllers and Administration & WebView Reporting, page 59
- Post-Installation Configuration: How to Configure Machines, page 62
- About the IPCC Web Administration Tool Deployment Wizard, page 62
- Initial Configuration: Machine Type Requirements, page 63
- How to Complete Deployment Wizard Pages, page 64
- Re-Accessing and Disabling the Deployment Wizard, page 68
- About Machine Roles, page 68
- Post-Installation Configuration: Create Additional IVR Connections and Grant System Permissions, page 69
- Post-Installation Configuration: Create Agents and Groups, page 70
- Post-Installation Configuration: Set Up Contact Routing, page 71

3rd Party Software: Prerequisite Installations

This section lists 3rd party software that must be installed, configured, or enabled prior to installing Controllers and Administration & WebView Reporting. These are in addition to the hardware, network, and operating system requirements described in the IPCC Enterprise Platform Specifications (page 19) section of this document.
Though not required, if you plan to use IPCC's optional SNMP monitoring feature, the Windows SNMP and WMI components must be enabled prior to installation.

SQLServer2000 must be installed as follows:
- Appropriate service pack as described in the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials*
- Configuration settings as described in the *Staging Guide for ICM/IPCC Enterprise and Hosted Editions*
- Named Pipes ordered before TCP IP (do this using the SQL Server Client Network utility)

The Windows IIS component must be installed.

For access to the IPCC Web Administration Tool, IE 6.0 sp1 or greater must be installed.

### 3rd Party Software: Packaged Software

The following 3rd party software is packaged and installed automatically with the Controllers and Administration & WebView Reporting:

<table>
<thead>
<tr>
<th>Software/Version</th>
<th>Installed On</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache Tomcat 5.0</td>
<td>Administration &amp; WebView Reporting</td>
<td>Servlet engine for the IPCC Web Administration Tool.</td>
</tr>
<tr>
<td>JDK 1.4.2_04</td>
<td>Administration &amp; WebView Reporting; Agent/IVR Controller</td>
<td>Java Development Kit.</td>
</tr>
<tr>
<td>New Atlanta Servlet Exec 5.0 ISAPI</td>
<td>Administration &amp; WebView Reporting</td>
<td>Servlet engine for WebView Reporting.</td>
</tr>
<tr>
<td>Sybase EAServer 5.1.0</td>
<td>Administration &amp; WebView Reporting</td>
<td>Translates reports to database queries for WebView Reporting.</td>
</tr>
</tbody>
</table>

**Note:** For information on whether subsequent version releases of this packaged software are supported with System IPCC, consult the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials.*
Installation Guidelines

After ensuring that all pre-installation prerequisites have been met for each machine on which you are installing IPCC, you can proceed with the System IPCC Enterprise installation.

**Note:** Always install the Controllers and Administration & WebView Reporting on a "clean" machine—that is, one which has a fresh install of the operating system and any prerequisite software. Under no circumstances should the Controllers or Administration & WebView Reporting be installed on a domain controller or DNS server.

IPCC components can be installed in any order. A suggested installation order would be:

- Central Controller
- Administration & WebView Reporting
- Agent / IVR Controller
- Optionally, the Outbound Controller
- Optionally, the Multichannel Controller. (Note: The Multichannel Controller is required only for deployments that include the multichannel options—CEM and/or CCS. If you are deploying both of these options, you must install, on separate machines, a Multichannel Controller for each.

**Note:** It is strongly recommended that you complete IPCC installation all on machines in your deployment before you begin configuring those machines. At minimum, a Central Controller and an Administration & WebView Reporting machine must be installed before any configuration is possible.

Installing and Configuring the Controllers and Administration & WebView Reporting

To install IPCC software for your controllers and Administration & WebView Reporting:

**Step 1** Login to the machine on which you want to install the first component using an Active Directory domain account. This account must have:

a. Administrative privileges to the local machine.

b. Permissions to create the IPCC Active Directory root Organizational Unit (OU) and facilities on your domain.

**Step 2** Insert the System IPCC Enterprise DVD in your machine's DVD drive.

**Step 3** Navigate to the top level of the System IPCC DVD.

**Step 4** Double-click setup.exe to launch the installer.
Step 5  At the Welcome screen, click Next.

Step 6  At the Set Up Machine Role screen, select the component set you want to install on this machine:

- All-in-One installs the System IPCC Central Controller, Agent/IVR Controller, Administration features, and WebView Reporting.
- Central Controller + Agent/IVR Controller installs the System IPCC Central Controller and Agent/IVR Controller.
- Central Controller installs the System IPCC Central Controller only.
- Agent/IVR Controller installs the System IPCC Agent/IVR Controller only.
- Administration & WebView Reporting installs System IPCC Administration features and WebView Reporting.
- Outbound Controller installs the System IPCC Outbound Controller which provides outbound dialing capability for the Outbound Option add-on.
- Multichannel Controller installs the System IPCC Multichannel Controller which provides a communication link between the Central Controller and the E-Mail Manager and/or Web Collaboration Option add-ons.

Step 7  At the Setup Type screen, specify whether this machine will be: simplex or side A of a duplexed deployment, OR side B of a duplexed deployment. Do not install a side B machine if you have not already installed its side A counterpart.

Step 8  Optionally, at the Security Hardening screen, specify whether or not you want to apply security hardening features to this machine.

**Note:** Security hardening applies Cisco recommended Windows hardening settings to your server, including settings for encryption, IPSec, NAT, and firewall configuration. See the Security Best Practices Guide for ICM and IPCC Enterprise and Hosted Editions for more information on IPCC security hardening.

Step 9  At the Start Copying Files screen, review the list of components to be installed and click Next to proceed or Back to modify your selections.

Step 10 The install begins. Certain stages of the install, particularly installation of WebView and the IPCC databases, may take some time to complete. This is normal behavior.

Step 11 After files complete copying, the IPCC Machine Initializer opens, in which you specify the Active Directory domain information for your deployment:

If this is the first machine on which you are installing IPCC, you will be prompted to create 1) the Cisco root for your domain, and 2) the facility under which this deployment will run.

If this is a subsequent machine installation, you will only need to select the appropriate AD facility from the list. All machines in your deployment must use the same facility.
**Note:** To create AD roots and facilities, you must have the appropriate privileges for your Active Directory domain. This means either that you are an AD administrator, or that the domain administrator has delegated you full control to this AD OU. See the *Staging Guide for ICM/IPCC Enterprise and Hosted Editions* for detailed information on deploying System IPCC Enterprise in Active Directory domains.

a. To create the Cisco root, in the IPCC Machine Initializer, under IPCC Root click Create.

b. Click on the + and the dialog shows all the Organizational Units in the domain. Select the OU you want the Cisco_Root to reside.

c. Click OK. The Cisco root--automatically named Cisco_ICM--is created.

d. To create the IPCC facility, under Create or Select Existing Facility click Create.

e. Enter a name for the facility.

f. Click OK.

**Step 12**
Click OK. The IPCC Machine Initializer creates the Active Domain entries, sets up the database rights and sets up registry and local accounts.

**Step 13**
If you installed an Agent/IVR Controller on this machine, install the JTAPI client on that machine as follows:

a. Open a browser window on the Agent/IVR Controller machine.

b. Enter the URL for the CallManager Administration utility: `http://<CallManager machine name>/ccmadmin`.

c. Choose Application > Install Plugins.

d. Click the icon next to Cisco JTAPI. A File Download box opens.

e. Choose Run this program from its current location. Click OK.

f. On the Security Warning box, click Yes to install.

g. Choose Next or Continue through the remaining Setup screens. Accept the default installation path.

h. Click Finish.

**Step 14**
Reboot the computer, logging in using the same account you used to install System IPCC Enterprise.

**Step 15**
Repeat the steps in this section to install System IPCC on the other machines in your deployment. When all installations are complete, proceed to the Post-Installation Configuration steps below.

**Note:** It is strongly recommended that you complete IPCC installation all on machines in your deployment before proceeding to configuring those machines. At minimum, a Central Controller
and an Administration & WebView Reporting machine must be installed before any configuration is possible.

**Post-Installation Configuration: How to Configure Machines**

After the Controllers and Administration & WebView Reporting have been installed on each machine in your deployment, use the Deployment Wizard in the IPCC Enterprise Web Administration Tool to set basic configuration information for each of these machines. This basic configuration sets system connection information, writes critical registry settings, and enables required services.

The Web Administration Tool is installed on the Administration & WebView Reporting machine. If your deployment includes two Administration & WebView Reporting machines, you can access the Web Administration Tool from either of these machines. However, it is still the case that only one of these machines is the "deployment master"—the machine from which other machines can be initially configured. In a deployment that includes two Administration & WebView Reporting machines, the wizard will prompt you to specify which of your Administration & WebView Reporting machines is the deployment master.

To access the IPCC Web Administration Tool:

- **Step 1**
  On any machine, open a Web browser (IE 6 or greater) and access the IPCC Enterprise Web Administration Tool at: https://<Administration & WebView Reporting machine DNS or IP Address>/ipccAdmin.

  The first time you access the IPCC Web Administration Tool you will be prompted to accept a self-signed security certificate. Install the certificate as follows:

  1. In the IE Security Alert dialog, click View Certificate.
  2. Click Install Certificate, then follow prompts to complete the installation.

  **Note:** See the Troubleshooting section of this document if you are prompted to accept a certificate subsequent to an initial login.

- **Step 2**
  On the Login page, enter the user name and password of the account you used to install System IPCC Enterprise. Password is case-sensitive.

**About the IPCC Web Administration Tool Deployment Wizard**

Immediately after installation, each machine in your deployment must be configured before it can be used in IPCC. The first time you access the IPCC Web Administration Tool after installing IPCC software it automatically displays the Deployment Wizard. The Deployment Wizard steps you through the process of configuring each controller and Administration & WebView Reporting
machine in your system (CallManager and IP IVR you configure separately, using the administration tools for those applications).

**Note:** Access to the Deployment wizard is limited to users with System Administrator privileges in the IPCC Web Administration Tool. The Active Directory user who installs the controller machines and Administration & WebView Reporting is automatically assigned System Administration privileges. Non-system administrators are presented a welcome page when they access IPCC Web Administration.

## Initial Configuration: Machine Type Requirements

The first machine to be configured is always the Administration & WebView Reporting machine on which you are running the Web Administration Tool. After that, the wizard will prompt you to configure, in order:

- Side A Central Controller
- Side B Central Controller (if deployed)
- Side A Agent/IVR Controller
- Side B Agent/IVR Controller (if deployed)
- Second Administration & WebView Reporting (if deployed)
- Outbound Controller (if deployed)
- Multichannel Controller for E-Mail Manager (if deployed)
- Multichannel Controller for Collaboration Server (if deployed)

Different machine types require different configuration. For each machine type, the Deployment Wizard displays in sequence the configuration pages that must be completed for each, as shown below:

<table>
<thead>
<tr>
<th>Machine Type</th>
<th>Configuration Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Controller</td>
<td>IPCC Network settings, Database settings</td>
</tr>
<tr>
<td>Agent/IVR Controller</td>
<td>IPCC Network settings, CallManager Connectivity settings, IVR Connectivity settings</td>
</tr>
<tr>
<td>Outbound Controller</td>
<td>IPCC Network Settings, CallManager Connectivity settings</td>
</tr>
<tr>
<td>Multichannel Controller</td>
<td>IPCC Network settings</td>
</tr>
<tr>
<td>Administration &amp; Reporting</td>
<td>IPCC Network settings, Database settings</td>
</tr>
</tbody>
</table>

Initial Configuration: Machine Type Requirements
How to Complete Deployment Wizard Pages

Wizard Page: Describe your IPCC Deployment

The first page in the Wizard prompts you to specify your deployment model. Complete its fields as follows:

**Step 1**<machine> is the Deployment Master: Check this if this Administration & WebView Reporting machine in your deployment will serve as the "deployment master"--the machine from which other machines will be configured. Only one Administration & WebView Reporting machine can be the deployment master. If you deselect the check box, the Wizard will terminate after the current machine is configured--thereafter, you must configure additional machines from the specified deployment master.

**Step 2** Disable the Deployment Wizard: Optionally, select this check box to permanently disable the Wizard after the current machine is created. Any machines that need to be added/configured subsequently must be done by running the Machine Wizard (from the Machines page). For this reason, it is recommended that only advanced users select this option.

**Step 3** Deployment: Select the deployment model you are using.

**Step 4** IPCC Options: Select any additional controllers you are deploying for optional components (Cisco E-Mail Manager, Cisco Collaboration Server, and Outbound Option). Note that while at installation there is only a single controller type for multichannel (CEM and CCS) options, you must install on separate machines a separate controller for each of these options you are deploying, and each must be configured separately.

**Step 5** Click Next. A message displays alerting you to the machine you will now configure.

Wizard Page: Describe the IPCC Machine in your Deployment

The second page in the Wizard prompts you to specify the role of the machine you are currently configuring. Complete its fields as follows:

**Step 1** Machine Hostname or IP Address: Enter the DNS or IP address of the machine you are configuring.

**Note:**
- For Administration & WebView Reporting machines and All-in-Ones IP addresses cannot be entered; you can enter a hostname only.
- If a connection to that machine cannot be made, or if the Wizard detects that the appropriate IPCC software has not been installed, you will be unable to proceed.
Step 2  Description: Optionally, include an internal description of this machine. This description will help you identify the machine when selecting for future actions within the IPCC Web Administration Tool.

Step 3  Role: Select the role this machine serves in your IPCC deployment. A default selection will already be made and in most cases this is what you should use. However, within certain limits, you have the ability to change the role of a machine. See the About Machine Roles section in this document for more information.

Step 4  Click Next.

Wizard Page: IPCC Network Settings

The third page in the Wizard prompts you to specify IPCC Network settings required for the machine you are currently configuring. Complete its fields as follows:

Step 1  If the machine you are configuring contains a Central Controller or Agent/IVR Controller, specify whether this machine type will be simplex or duplex in your deployment. Select Duplex if two physical machines (side A and side B) will each run the IPCC software.

Note: When setting up a standalone Central Controller in a duplexed environment, the first Central Controller must be set to Simplexed at initial configuration. After the second Central Controller is configured, you can then return to the first and set it to Duplex.

Step 2  Provide network addresses, as fields indicate. Depending on the machine type you are configuring, you may need to provide: A) both public and private addresses for B) both side A and side B for both the Central Controller and Agent/IVR Controller.

When completing these fields:

- Public Hostname = The visible network address of the Side A machine. You can enter either the machine's DNS or IP address.

- Private Hostname = The private network address of the Side A machine. You can enter either the machine's DNS or IP address.

- If you are deploying a simplex system, the value in side B fields can either be left blank or must be identical to the values for side A. For a duplexed environment, specify different addresses for the side A and B machines.

Step 3  If the machine you are configuring contains an Agent/IVR Controller, select Collect Agent and Skill Group Statistics if you want to allow real-time agent and skill group data to be displayed in agent desktops. You can also modify the default collection interval for skill group data. Enabling agent reporting automatically disables Quality of Service for the CTI Server.

Step 4  Reboot Machine on Error causes IPCC to automatically initiate a reboot in the event of a critical error. This option is selected by default. In a duplexed environment, rebooting on error will keep the system up if only one of the sides fail. Do not deselect Reboot Machine on Error unless specifically told to do so by Customer Support.
Step 5  Do not deselect Reboot Machine on Request unless specifically told to do so by Customer Support. Turning off this option prevents the machine from rebooting, even if it detects a serious system-wide problem.

Step 6  Optionally, for deployments that use the Mobile Agent option, the codec to be used for both incoming customer and outgoing Mobile Agent calls. For more information on codec selection see the Mobile Agent Guide for Cisco Unified CC Enterprise & Hosted.

Step 7  Optionally, select the type of type of supervisor Silent Monitoring you will use in your deployment. If you select Disabled, CTI OS-based silent monitor will be configured, but disabled. For more information on silent monitor setup see the CTI OS System Manager’s Guide.

Step 8  Optionally, use the QoS link(s) to enable the Cisco Quality of Service (QoS) feature.

Set DSCP (DiffServ Codepoint) and 802.1p priority tagging as appropriate and allowed. The defaults are acceptable if your network is Cisco AVVID compliant. Otherwise, consult your network administrator or Cisco representative for the proper values for these fields.

See the ICM Pre-installation Planning Guide for Cisco ICM Enterprise Edition and the IPCC Enterprise Solution Reference Network Design (SRND) Guide for information on implementing Cisco QoS, including calculating bandwidth requirements and important information on using it with Microsoft Packet Scheduler.

Step 9  If you are configuring a standalone Administration & WebView Reporting machine, specify the Preferred Central Controller as follows:

In a duplexed deployment that includes two standalone Administration & WebView Reporting machines, set each to use a different preferred Central Controller. Doing this provides protection against potential data replication issues resulting from failover.

In a simplexed deployment, or if your deployment includes only one Administration & WebView Reporting machine, set the preferred Central Controller to the Side A machine.

Step 10  Click Next.

Step 11  If the machine you are currently configuring is a Multichannel Controller, Click Finish. The machine will now be configured and the appropriate IPCC services started on it. When that process is complete, the Wizard will prompt you to configure the next machine in your deployment.

If the current machine is not a Multichannel Controller, proceed to Wizard Page: Call Manager Connectivity Settings.

Wizard Page: Call Manager Connectivity Settings

If the machine you are currently configuring includes an Agent/IVR Controller or an Outbound Controller, the next page to display prompts you for information on your Call Manager. (If you are not configuring an Agent/IVR or Outbound Controller, proceed to Wizard Page: Database Settings.)
On the Call Manager Connectivity Settings page, complete the following:

**Step 1** Call Manager Machine Hostname or IP Address: Enter the DNS or IP address of the Call Manager machine in your deployment; or, for Outbound Option, the CallManager TFTP Server.

**Step 2** If the machine you are working with is an Agent/IVR Controller, enter or modify the following additional fields:

- **Call Manager Agent Extension Length**: Enter the Call Manager extension length you entered when you configured Call Manager. Defaults to 7.
- **Call Manager JTAPI User ID and Password**: Enter the user ID and password of the JTAPI user you created when configuring Call Manager.

**Step 3** Click Next.

**Step 4** If the machine you are currently configuring is an Outbound Controller, Click Finish. The machine will now be configured and the appropriate IPCC services started on it. When that process is complete, the Wizard will prompt you to configure the next machine in your deployment.

If the current machine is not an Outbound Controller, proceed to Wizard Page: IVR Connectivity Settings.

---

**Wizard Page: IVR Connectivity Settings**

If the machine you are currently configuring includes an Agent/IVR Controller, the next page to display prompts you for information on your IP IVR.

On the IVR Connectivity Settings page, complete the following:

**Step 1** Click Enable to enable the IP IVR within the IPCC deployment.

**Step 2** **IVR Machine Hostname or IP Address**: Enter the DNS or IP address of the IP IVR machine in your deployment.

**Note:** If you are deploying multiple IP IVRs, additional IP IVRs can be added later via the IVR Connectivity page.

**Step 3** **IVR Connection Port Number**: Enter the VRU Connection Port number specified in the CRS Administration Tool when your IP IVR was configured. This defaults to 5000, the same default port that IP IVR uses.

**Step 4** Click Next.

**Step 5** Click Finish. The machine will now be configured and the appropriate IPCC services started on it. When that process is complete, the Wizard will prompt you to configure the next machine in your deployment.
Wizard Page: Database Settings

If the machine you are currently configuring includes a Central Controller or Administration & WebView Reporting, the next page to display prompts you for IPCC database maintenance information.

IPCC can initiate a purge process on the Central Controller and Administration & WebView Reporting machine according to a set schedule. The purge process deletes records that are older than a specified number of days. By default, the purge process runs each night at 12:30 A.M.

On the Database Settings page, accept the default value or complete the following:

Step 1: In Database Purge Schedule, indicate the time and days on which you want the purge job to execute.

Step 2: Click Next.

Step 3: Click Finish. The machine you are working with will now be configured and the appropriate IPCC services started on it. When that process is complete, the Wizard will prompt you to configure the next machine in your deployment.

Re-Accessing and Disabling the Deployment Wizard

The Deployment Wizard displays automatically the first time you access the IPCC Web Administration Tool after installing IPCC. It will continue to display in the Web Administration Tool until every machine in your deployment has been configured. After that, it will never display. Until then, you can also access it by clicking the Run Deployment Wizard button on the Machines page.

Experienced users, familiar with the configuration requirements for each IPCC machine type, may prefer to configure machines independent of the Deployment Wizard. To allow this, the first screen of the Deployment Wizard includes a Disable Deployment Wizard check box. Checking this box will permanently disable the Deployment Wizard. There is also a Disable Deployment Wizard button on the Machines page. Choose carefully when selecting this option—once selected, the Deployment Wizard will be permanently unavailable. The button on the Machines page that can be used to access it after initial configuration will no longer appear.

About Machine Roles

A System IPCC role must be assigned to each controller machine and Administration & WebView Reporting machine in your system. Typically this is done when the Deployment Wizard is run immediately after installation. However, if you prefer not to use the Deployment Wizard for initial configuration, or if you need to modify the role or settings of a machine, or if you need to add a new machine to your deployment, you can do so through the Machines Wizard in the IPCC Web Administration Tool.
For machines that already have an assigned role, you can modify roles within the limits of the rules listed below. Typically, changing a machine role would only be done in the course of growing your deployment model. If the machine was installed as:

- A standalone Administration & WebView Reporting machine, the role cannot change.

- An Agent/IVR Controller or an Outbound or Multichannel Controller, the role can only be changed to one of those three.

- A Central Controller or a Central Controller + Agent/IVR Controller, the role can only be changed to one of those two.

- An All-In-One, it can change to a Agent/IVR Controller+Central Controller or a standalone Central Controller, but with a warning that it cannot subsequently be changed back. You cannot make this change if you are running the IPCC Web Administration Tool on the All-In-One you are attempting to change. You would first need to install a standalone Administration & WebView Reporting machine, and then make the change from the Web Administration Tool running on that machine.

Post-Installation Configuration: Create Additional IVR Connections and Grant System Permissions

Perform the tasks listed below to create, as necessary, connections to additional IP IVRs in your system and to grant user permissions to the IPCC Web Administration Tool and WebView Reporting.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>IPCC Web Administration Tool Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create IVR Connections; Configure the Network IVR</td>
<td>Once IPCC software has been installed, connection information to any additional IP IVR(s) in your deployment must be specified in the IPCC Web Administration Tool. Also, the Network IVR (which serves as a virtual IVR connection to multiple physical IVRs) must be configured.</td>
<td>IVR Connectivity page; Network IVR page</td>
</tr>
<tr>
<td>Assign IPCC system privileges. Assign WebView Reporting access.</td>
<td>There are three levels of IPCC privilege: System Administrator; Administrator; and WebView User. All require that the prospective user first have an Active Directory account on IPCC’s AD domain. System Administrators and (Contact Center) Administrators both have access to the IPCC Web Administration Tool, with System Administrators having access to a wider range of pages. WebView users have access to WebView Reporting. Note: Agent supervisors can also be given access to WebView (via the Agents page) their access will be limited to reports on the agent teams they supervise.</td>
<td>Administrative Permissions page</td>
</tr>
</tbody>
</table>
Post-Installation Configuration: Create Agents and Groups

Perform the tasks listed below to create agent records and agent groupings for your IPCC system. Tasks do not need to be performed in the order shown below; however, this order offers expediency as it reflects dependencies of certain record types on the pre-existence of others.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>IPCC Web Administration Tool Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Agent Desk Settings.</td>
<td>Agent Desk Settings associate a set of permissions or characteristics with specific agents, such as how and when calls to these agents are redirected, how and when they enter various works states, and whether they can make outbound calls. You can create a Default Desk Setting that is the set of permissions automatically assigned to all new agents unless overridden.</td>
<td>Agent Desk Settings page</td>
</tr>
<tr>
<td>Create Agents and Agent Supervisors. Assign desk settings to agents. Give supervisors WebView access.</td>
<td>In order to use IPCC, all prospective agents first need an account which includes a login ID and password. You can designate certain agents as supervisors, allowing them to be later designated as supervisors of agent teams. Supervisors—provided they have an Active Directory account on IPCC's AD domain—can be given access to WebView Reporting. You can assign different desk settings to different agents based on their needs, and, as necessary, temporarily suspend their login privileges or turn on Agent State Trace, which allows you to track their transition through various states of readiness.</td>
<td>Agents page</td>
</tr>
<tr>
<td>Create Skill Groups and assign agents to skill groups.</td>
<td>A skill group is a collection of agents that share a common set of skills. In IPCC, skill groups are one of the primary devices for routing and reporting. An agent can be associated with multiple skill groups and each skill group is associated with a specific media routing domain (MRD) such as voice, chat, or e-mail. Note that the IPCC Web Administration Tool allows you to create, view, and assign agents to Voice skill groups only. If you are deploying other MRD options, skill groups associated with those MRDs must be administered via the Administration interfaces for those applications.</td>
<td>Skill Groups page</td>
</tr>
<tr>
<td>Create Agent Teams. Assign agents and supervisors to teams.</td>
<td>Agent teams allow you to associate a set of agents with a specific supervisor. In addition to reporting uses, this association also allows IPCC to determine which supervisor to route an agent's Supervisor Assist requests to.</td>
<td>Agent Teams page</td>
</tr>
</tbody>
</table>
Post-Installation Configuration: Set Up Contact Routing

Perform the tasks listed below to configure contact (voice and non-voice) routing for your IPCC system. Tasks do not need to be performed in the order shown below; however, this order offers expediency as it reflects dependencies of certain record types on the pre-existence of others.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>IPCC Web Administration Tool Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optionally, create Enterprise Skill Groups. Assign skill groups to enterprise skill groups.</td>
<td>An enterprise skill group is a logical grouping of skill groups, and can include skill groups from different MRDs. Through enterprise skill groups, you can generate reports that include any grouping of skill groups you desire. Note: Unlike the Skill Groups page, the Enterprise Skill Groups page in IPCC Web Administration can display skill groups from all MRDs.</td>
<td>Enterprise Skill Groups page</td>
</tr>
</tbody>
</table>

### Call Types page

A call type is a category of incoming routable task. Specific call types are associated with Dialed Numbers. In this association, each call type has a schedule that determines which routing script(s) are active for that call type at any time. Because the call type determines which routing script is run for a call, the call type defines call treatment in an IPCC Enterprise system.

There are two classes of call type/dialed number associations: voice and non-voice.

### Dialed Numbers page

In IPCC, you set up a Dialed Number List, which identifies all of the phone numbers in your contact center that customers can dial to initiate contact. Dialed numbers are mapped to call types; this mapping is used to identify the appropriate routing script for each call.

A typical call center requires a number of dialed number definitions. In addition to answered calls, dialed numbers also need to be set up for ring on no answer, dialed number plan entries, and for supervisor/emergency assist calls.

### Call Variables page; User Variables page; Application Gateway page; Database Lookups page

As desired, you can create IPCC Call and User variables that can then be used to pass call and user data to routing scripts.
### Task Description

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>IPCC Web Administration Tool Location</th>
</tr>
</thead>
</table>
| Optionally, identify IVR Scripts. | As desired, identify scripts used by your IVR so that IPCC can interact with them.  

**Note:** IVR scripts should be tagged as "Interruptible." This allows a script to be interrupted once a routing target becomes available. If not so tagged, a call queued in the IVR will not be transferred until the script completes, even if the agent becomes available beforehand. | IVR Script page |
| Install Internet Script Editor; Create IVR scripts, IPCC routing and administration scripts, and multichannel scripts | After you have completed your IPCC configuration in the IPCC Web Administration Tool, you can write IVR scripts, IPCC routing and administrative scripts, and as necessary, scripts for your multichannel applications:  
- An IVR script is a routing script that controls voice treatment activity on an IVR (in System IPCC, your IVR product is IP IVR). The content of the voice treatment activity is entirely determined by the IVR. It can be as simple as playing a single recorded announcement or as complex as an entire self-service operation.  
- An IPCC routing script processes call routing requests from a routing client. Typically it examines several targets and applies selection rules to find an available qualified agent or a target with the shortest expected delay. You can set up different routing scripts to execute for different types of tasks. You can define call types in terms of the telephone number the caller dialed, the number the caller is calling from, and additional digits entered by the caller. For each call type, you can schedule different routing scripts to execute on different days or at different times of the day. An  
- An IPCC administrative script runs periodically to perform a task, such as setting variables. | Create IVR scripts (for IP IVR) using the CRA Editor application.  
Create IPCC routing and administration scripts using the Internet Script Editor application (or its local-access version on the Administration & WebView Reporting machine), Script Editor.  
You can install Internet Script Editor on any client machine that can access the IPCC Web Administration Tool. To install Internet Script Editor on a client machine: 1) From the client machine, login to IPCC Web Admin; 2) On the Downloads page, download the Script Editor installer; 3) Run the installer on the client.  
Scripts for use with multichannel (Cisco Collaboration Server and Cisco E-Mail Manager) and/or outbound options typically require additional setup in the administration interfaces for these products.  
For detailed information on creating and deploying scripts for IPCC, see the *ICM Scripting and Media Routing Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* (for IPCC routing and administration scripts), the *Cisco Customer Response Applications Editor Step Reference Guide* (for IVR scripts), and your multichannel and outbound option documentation. |
Installing Agent and Supervisor Desktop Software for IPCC Enterprise

This section provides information on installing agent and supervisor desktop software for IPCC Enterprise. To provide agent and supervisor desktop software, you can deploy either Cisco CTI OS or Cisco Agent Desktop (CAD)/Cisco IPCC Supervisor Desktop with IPCC Enterprise.

**Note:** This guide does not describe post-installation configuration of CTI OS and CAD desktops. For that information, see the IPCC Administration Guide for Cisco IPCC Enterprise Edition.

The following Cisco documents provide more detailed information on the installation/configuration tasks described in this section:

- *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*
- *Cisco Agent Desktop (CAD) Installation Guide*
- *IPCC Administration Guide for Cisco IPCC Enterprise Edition*

This section contains the following topics:

- **About Agent and Supervisor Desktops for IPCC Enterprise**, page 73
- **About the CTI Server and the CTI OS Server**, page 74
- **About Agent and Supervisor Desktop Installation Prerequisites**, page 74
- **How to Install CTI OS**, page 75
- **How to Install and Configure the Cisco Agent Desktop Applications**, page 77

**About Agent and Supervisor Desktops for IPCC Enterprise**

Cisco Computer Telephony Integration (CTI OS) and Cisco Agent/Supervisor Desktop (CAD) are server-based CTI solutions that provide desktops used by contact center agents and
supervisors. Both desktop packages are supported by IPCC. You deploy one or the other in your IPCC system:

- CTI OS includes the CTI OS Server, CTI OS Agent Desktop, IPCC Supervisor Desktop, CTI OS Toolkit, and Client Interface Library (CIL). It provides an object-oriented software development toolkit for development and deployment of CTI applications.

- Cisco Agent/Supervisor Desktop (CAD) includes the Desktop Administrator, Agent Desktop, and Supervisor Desktop.

**About the CTI Server and the CTI OS Server**

Regardless of which agent desktop software you deploy--CAD or CTI OS--both communicate to IPCC via the CTI server--a software process that runs on the Agent/IVR Controller. The CTI Server is the CTI gateway into IPCC’s data and services. It allows IPCC to deliver agent, call, and customer data in real-time to a server and/or workstation application as events occur throughout the life of a call.

Both also require the CTI OS Server. The CTI Server and CTI OS Server are both installed automatically and reside on your Agent/IVR Controller. No manual installation or configuration of these components is necessary.

**About Agent and Supervisor Desktop Installation Prerequisites**

Before installing and configuring agent and supervisor desktop software for use with IPCC Enterprise, you must:

<table>
<thead>
<tr>
<th>Desktop Installation Prerequisite</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install and configure Cisco CallManager</td>
<td></td>
</tr>
<tr>
<td>Install and configure IP IVR</td>
<td></td>
</tr>
<tr>
<td>Install and configure the controllers and Administration &amp; WebView Reporting</td>
<td></td>
</tr>
<tr>
<td>Create agents, supervisors, and teams</td>
<td></td>
</tr>
<tr>
<td>If you are deploying CTI OS and want to use the CTI OS Silent Monitoring feature...</td>
<td>CTI OS includes a Silent Monitor feature, which enables a supervisor to listen to an agent’s call by forwarding voice traffic from an agent’s phone</td>
</tr>
</tbody>
</table>
How to Install CTI OS

CTI OS incorporates the CTI OS Server, the CTI OS Toolkit, Agent Desktop, Supervisor Desktop and Client Interface Library. Step-by-step installation instructions for CTI OS are included in the CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions.

Note: The CTI OS Server is installed automatically and resides on your Agent/IVR Controller. No manual installation or configuration of this components is necessary.

How to Install the CTI OS Supervisor Desktop

Warning: CTI OS uses certificates (self-signed or third-party) for authentication between the CTI OS server and desktop clients. Before you install the supervisor desktop, you must know which (self-signed or third party) certificate type your company uses. After you install the supervisor desktop, you will need to copy key and request files from the client to the CA machine, sign them, and then return signed files to the client. If you are not already familiar with the CTI OS certificate signing procedures used at your company, please consult you CTI OS administrator or the CTI OS System Managers Guide before proceeding with desktop software installation.

To install the CTI OS Supervisor Desktop, complete these steps:

**Step 1**
Open a browser on the client machine where you want to install the software and log into the IPCC Web Administration Tool.

**Note:** Access IPCC Web Administration at: https:<Administration & WebView Reporting machine IP or DNS name>/ipccAdmin. You will need to login using an account that has Administrator or System Administrator privileges for IPCC.

**Step 2**
Go to System Management Pages > Downloads.
Step 3  Click the link for the CTIOSClient.zip file and select Save to download the file.

Step 4  After the download is complete, unzip the file and double-click setup.exe to launch the installer.

Step 5  Click Yes on the Software License Agreement screen.

Step 6  On the Destination Location screen, accept the default installation directory or click the Browse button to specify another directory. Click OK.

Step 7  On the Select Components screen, select IPCC Supervisor Desktop. Click Next.

Step 8  On the CTI OS Server Information screen, enter the name or IP address for your Agent/IVR Controller. Accept the default Port number 42028. Click Next.

Step 9  Click Next to start the installation.

Step 10  In the Client Security dialog, select the Certificate Authority type used by your company. Enter a security password 8-30 characters long. Click OK.

Note: Record this password. You will need to provide it when the certificate request file from this client is signed on the CA machine.

Step 11  The next screen displays further actions that must be taken to sign files based on the Certificate Authority type. Please review this information if you are unfamiliar with it. Click Next.

Step 12  When the installation of files is complete, Click Finish.

Step 13  Reboot the machine to complete the installation.

How to Install the CTI OS Agent Desktop

Warning: CTI OS uses certificates (self-signed or third-party) for authentication between the CTI OS server and desktop clients. Before you install the supervisor desktop, you must know which (self-signed or third party) certificate type your company uses. After you install the supervisor desktop, you will need to copy key and request files from the client to the CA machine, sign them, and then return signed files to the client. If you are not already familiar with the CTI OS certificate signing procedures used at your company, please consult you CTI OS administrator or the CTI OS System Managers Guide before proceeding with desktop software installation.

To install the CTI OS Agent Desktop, complete these steps:

Step 1  Open a browser on the client machine where you want to install the software and log into the IPCC Web Administration Tool.

Note: Access IPCC Web Administration at: https://<Administration & WebView Reporting machine IP or DNS name>/ipccAdmin. You will need to login using an account that has Administrator or System Administrator privileges for IPCC.
Step 2 Go to System Management Pages > Downloads.

Step 3 Click the link for the CTIOSClient.zip file and select Save to download the file.

Step 4 After the download is complete, unzip the file and double-click setup.exe to launch the installer.

Step 5 Click Yes on the Software License Agreement screen.

Step 6 On the Destination Location screen, accept the default installation directory or click the Browse button to specify another directory. Click OK.

Step 7 On the Select Components screen, select Agent Desktop. Click Next.

Step 8 On the CTI OS Server Information screen, enter the name or IP address for your Agent/IVR Controller. Accept the default Port number 42028. Click Next.

Step 9 Click Next to start the installation.

Step 10 In the Client Security dialog, select the Certificate Authority type used by your company. Enter a security password 8-30 characters long. Click OK.

Note: Record this password. You will need to provide it when the certificate request file from this client is signed on the CA machine.

Step 11 The next screen displays further actions that must be taken to sign files based on the Certificate Authority type. Please review this information if you are unfamiliar with it. Click Next.

Step 12 When the installation of files is complete, Click Finish.

Step 13 Reboot the machine to complete the installation.

How to Install and Configure the Cisco Agent Desktop Applications

Cisco Agent Desktop (CAD) Pre-Installation Requirements

For Cisco Agent Desktop applications to work properly, your agents must be organized into teams and some must be designated as supervisors. Create agents, teams, and supervisors in IPCC (using the IPCC Web Administration Tool) before you install Cisco Agent Desktop software.

Use the following worksheet to assemble the configuration information required during CAD installation. Depending on your configuration, you may not need to complete every section of the worksheet.

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Directory Services</td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Logical contact center name</td>
<td></td>
</tr>
<tr>
<td><strong>Secondary Directory Services</strong></td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td><strong>Base Services</strong></td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td><strong>Recording &amp; Playback service(s)</strong></td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>VoIP Monitor Service(s)</strong></td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CallManager (Publisher)</strong></td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td><strong>CallManager (Subscribers)</strong></td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CallManager Database</strong></td>
<td></td>
</tr>
<tr>
<td>CallManager version</td>
<td></td>
</tr>
<tr>
<td>Database login ID</td>
<td></td>
</tr>
<tr>
<td><strong>Item</strong></td>
<td><strong>Value</strong></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Database password</td>
<td></td>
</tr>
<tr>
<td><strong>IPCC SQL Logger Database</strong></td>
<td>(Located on Central Controller)</td>
</tr>
<tr>
<td>Instance name</td>
<td></td>
</tr>
<tr>
<td>Login ID</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td><strong>Side A</strong> Host name / IP address</td>
<td></td>
</tr>
<tr>
<td><strong>Side B</strong> Host name / IP address</td>
<td></td>
</tr>
<tr>
<td><strong>CTI Service Associated with CallManager</strong></td>
<td></td>
</tr>
<tr>
<td>Peripheral ID</td>
<td></td>
</tr>
<tr>
<td><strong>Side A</strong> Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td><strong>Side B</strong> Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td><strong>CTI Service Associated with IP IVR</strong></td>
<td></td>
</tr>
<tr>
<td>Peripheral ID</td>
<td></td>
</tr>
<tr>
<td><strong>Side A</strong> Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td><strong>Side B</strong> Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td><strong>CTI OS (Server 1)</strong></td>
<td>(Located on Agent/IVR Controller)</td>
</tr>
<tr>
<td>Peripheral ID</td>
<td></td>
</tr>
</tbody>
</table>
How to Install and Configure the Cisco Agent Desktop Applications

To install Cisco Agent Desktop, follow the step-by-step installation instructions included in the *Cisco Agent Desktop Installation Guide*.

CAD components must be installed in this order:

1. Services
2. Desktop Administrator
3. Supervisor Desktop and Agent Desktops

CAD Services and the Desktop Administrator are installed from the CAD CD. The CAD Configuration application runs automatically after you install the services and Desktop Administrator on the CRS server. Following that, you can change your configuration settings by launching the Desktop Administrator.
The Supervisor and the Agent Desktops are installed from the Web server on which the CAD services are installed.

**Note:** It's important to communicate to CAD agents and supervisors that they must login to their CAD desktop application using their Login Name, not an Agent ID. System IPCC Enterprise does not support desktop login using an Agent ID.

**See Also**

*Cisco Desktop Administrator User's Guide*
Chapter 8: Installing Agent and Supervisor Desktop Software for IPCC Enterprise

How to Install and Configure the Cisco Agent Desktop Applications
Chapter 9

Installing and Configuring Outbound Option for IPCC Enterprise

This section describes how to configure the optional Outbound Option feature for IPCC Enterprise.

Note: This guide does not describe how to create dialing campaigns for Outbound Option. For that information, see the Outbound Option User Guide for Cisco ICM/IPCC Enterprise & IPCC Hosted Editions.

This section contains the following topics:

- About Outbound Option, page 83
- How to Install Outbound Option for IPCC Enterprise, page 84
- Outbound Option Configuration Tasks, page 84
- How to Configure Outbound Option Dialers, page 84
- How to Configure General System Time Options, page 85
- How to Enable Call Variables for Outbound Option, page 85
- How to Configure the Transfer to IVR Feature, page 86
- How to Configure CallManager for Outbound Option, page 86
- About Scripting for Outbound Option, page 88

About Outbound Option

Outbound Option is a feature of IPCC that provides outbound dialing functionality along with the existing inbound capabilities of IPCC. With Outbound Option, contact centers can be configured for automated outbound activities. Agents who are not busy handling inbound requests can perform outbound calls, thereby maintaining a high level of agent productivity.

For IPCC Enterprise, a Cisco voice gateway is required to place customer calls.
How to Install Outbound Option for IPCC Enterprise

You install Outbound Option by installing the Outbound Controller as described in Installing and Configuring the Controllers and Administration & WebView Reporting (page 57).

Note: IPCC automatically installs Outbound components to your deployment's side A Central Controller. These components are then enabled if and when you add an Outbound Controller to the deployment.

Outbound Option Configuration Tasks

After you install Outbound Option, complete these tasks to configure it for use with IPCC. Perform tasks in the order listed. Instructions for each are included later in this section.

<table>
<thead>
<tr>
<th>CallManager Configuration Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure the dialer.</td>
<td></td>
</tr>
<tr>
<td>2. Disable MTP Required option if you are using Call Progress Analysis (CPA).</td>
<td></td>
</tr>
<tr>
<td>3. Configure General System Time Options.</td>
<td></td>
</tr>
<tr>
<td>4. Enable Outbound Option Call Variables</td>
<td></td>
</tr>
<tr>
<td>5. Create a transfer to IVR campaign if you are using the transfer to IVR feature.</td>
<td></td>
</tr>
<tr>
<td>6. On the CallManager, configure port devices, call waiting, and music on hold.</td>
<td></td>
</tr>
<tr>
<td>7. Create Outbound Option Scripts.</td>
<td></td>
</tr>
</tbody>
</table>

How to Configure Outbound Option Dialers

All dialers used in the Outbound Option system must be configured through the Outbound Option Dialer Configuration Component option in the IPCC Configuration Manager. IPCC Configuration Manager is accessible from the IPCC Admin program group on your Administration & WebView Reporting machine.

To configure the Outbound Option dialer:
Step 1  In IPCC Configuration Manager, select Outbound Option > Dialer.

Step 2  Click the Retrieve button.

Step 3  Click the Add button to add a new Dialer.

Step 4  Complete the fields on the Dialer General tab.

Step 5  Click the Port Map Selection tab to begin adding ports to the Dialer.

Note: This specifies the number of ports available on the Dialer and the extension numbers, which the CallManager assigns to those ports. The maximum number of ports per Dialer is 96. Each configured port represents a Dialer phone device on CallManager. These Dialer phone devices carry a greater device weight than standard IP telephones.

Step 6  Enter the port number range.

Step 7  Click Save to save all the configuration information.

How to Configure General System Time Options

To comply with regulations concerning what time contacts might be called, specify the General System Time options. This time range entered here applies to all campaigns which the Outbound Option system will run, and supersedes any individual campaign time ranges. This guarantees that a contact is not called before or beyond a particular time. Outbound Option automatically converts the times specified to the contact's local time.

To configure the system time options:

Step 1  In the IPCC Configuration Manager, double-click the Outbound Option - System Options option from the drop-down list.

Step 2  Enter values for the customer dialing time range, as desired.

Step 3  Click OK to save the changes.

How to Enable Call Variables for Outbound Option

Enable the Outbound Option call variables using Call Variables page in the IPCC Web Administration Tool. To enable the Outbound Option call variables:

Step 1  In the IPCC Web Administration Tool select Contact Management > Call Variables.

Step 2  Enable the Enable expanded call context check box.

Step 3  One-by-one, open all BAxxxx variables (BAAccountNumber, BABuddyName, BACampaign, BADialedListID, BAResponse, BStatus, and BAResponse).
How to Configure the Transfer to IVR Feature

**Step 4**  
Click the Enabled check box.

**Step 5**  
Click Save.

How to Configure the Transfer to IVR Feature

If you are using the transfer to IVR feature, create a transfer to IVR campaign following the instructions in the *Outbound Option User Guide for Cisco ICM/IPCC Enterprise & IPCC Hosted Editions*. When using this feature, note that Outbound Option only supports IP IVR Type 2.

**Note:** The transfer to IVR feature is only supported for Outbound Option on Cisco IP Contact Center (IPCC Enterprise). You can not use this feature in the Direct Preview or the regular Preview modes.

Transfer to IVR campaigns might require translation routes if using a Type 2 IVR.

How to Configure CallManager for Outbound Option

After you have configured the Outbound Option feature in IPCC you must return to Cisco CallManager to configure port devices for the Outbound Option Dialer and configure music on hold for Outbound Option devices.

How to Configure the Outbound Option Port Devices

After creating a dialer port map in IPCC for Outbound Option, you must create dialer port devices using Cisco CallManager.

To create Dialer Port Devices in Cisco CallManager:

**Step 1**  
After configuring the Dialer Port Map (in Configuration Manager), click the Export button to save the port map configuration to a CSV-formatted test file, such as DialerportExport.CSV.

**Step 2**  
Using the CallManager Bulk Administration Tool (choose Application > BAT), create a new phone template. (Cisco CallManager BAT must first be installed. You can install BAT from the Cisco CallManager Install Plugins page.) Choose the Cisco 30 VIP phone option, set the device pool, and choose the Default 30 VIP phone button template.

**Step 3**  
Insert a single line with no speed dials.

**Step 4**  
Copy the exported CSV file to the BAT phone directory on the publisher CallManager (typically C:\Batfiles\Phones).

**Step 5**  
Using BAT, choose Configure Phones and select the exported CSV file and newly created phone template to import the file and create the new devices.
Step 6  Associate the newly created devices with the JTAPI user that you created for the Agent/IVR Controller:
   a. From the CallManager Administration page, choose User > Global Directory and click Search.
   b. Click the Agent/IVR Controller JTAPI user that you created. Click Device Association.
   c. In the Device List Filter, select Directory Number and enter the first few digits of the newly created dialer ports.
   d. Click Select Devices. Make sure the check box next to each dialer port is checked.

Step 7  Click Update.

Note: Make sure the CallManager Call Waiting option is enabled on each outbound agent phone. If the Call Waiting option is not enabled, every customer call transferred to an agent will fail. (CallManager Release 4.0(0) and later users do not need to enable this option since it is enabled by default.)

How to Enable the CallManager Call Waiting Option on Outbound Agent Phones

The Call Waiting option must be enabled in CallManager on each outbound agent phone to ensure that every customer call successfully transfers to an available agent.

Note: CallManager Release 4.0(0) and later users do not need to enable this option since it is enabled by default.

To enable the Call Waiting option:

Step 1  From the CallManager Phone Configuration window, select Line 1.

Step 2  In the Directory Number Settings submenu, select the On option in the Call Waiting pull-down selection box.

Step 3  Click Update to save the changes.

How to Configure Music on Hold

Once Outbound has an established customer call, the call is placed on hold for a short time (usually a sub-second) before being transferred to an agent. During this time, the customer might hear a set of tones indicating that the call has been placed on hold.

Step 1  Configure Cisco CallManager to play music while on hold for the device pool containing the Outbound Option Dialer port devices.
Step 2  Use a short (about 5 seconds) blank sound file to ensure that the customer does not hear anything during the short time period before the call is transferred.

About Scripting for Outbound Option

For Outbound Option, you must create:

- A routing script that uses the dialed number for the MR routing client and routes through a Select node to previously configured skill groups.

- An administrative script for each skill group to control the Outbound Control variable and the skill group reservation percentage.

Instructions for writing scripts for Outbound Option are provided in the Outbound Option Setup and Configuration Guide for Cisco ICM/IPCC Enterprise & IPCC Hosted Editions and the Outbound Option User Guide for Cisco ICM/IPCC Enterprise & IPCC Hosted Editions.

When writing scripts for Outbound Option, you must consider two variables:

- The Outbound Control Variable

- The Outbound Percent Variable

About the Outbound Control Variable

The Outbound Option Dialer looks for an Outbound Control variable to understand the mode for each skill group. You must supply one of the following outbound control values when you create an administrative script using the Internet Script Editor application:

- INBOUND. Indicates that this skill group is disabled for outbound use and only takes inbound calls.

- PREDICTIVE_ONLY. Dials several customers per agent. After reaching a live contact, the Predictive Dialer transfers the customer to a live agent along with a screen pop to the agent's desk. The predictive algorithm is designed to calculate the number of lines to dial per available agent to keep agent wait time to a minimum.

- PREDICTIVE_BLENDED. Agents receive inbound calls, but could be used for an outbound call when available.

- PREVIEW_ONLY. Reserves an agent prior to initiating an outbound call and presents the agent with a screen pop. The agent might then:
  - Accept the call: Dials the customer and transfers the call to the agent
  - Skip the call: Agent receives another customer call.
Reject the call: Releases the agent. At this point, the system might deliver the agent another preview outbound call or a new inbound call.

- **PREVIEW_BLENDED.** Agents receive inbound calls, but could be used for an outbound preview call when available.

- **PROGRESSIVE_ONLY.** Similar to PREDICTIVE_ONLY; however, lines to dial per agent are not calculated—users configure a fixed number of lines that will always be dialed per available agent.

- **PROGRESSIVE_BLENDED.** Similar to PREDICTIVE_BLENDED; but a fixed number of lines are always dialed per available agent.

### About the Outbound Percent Variable

Set the Outbound Percent variable in the same administrative script; for example, select the Outbound Percent variable in the Set Properties window and enter the agent percentage in the Value field. This variable controls the percentage of agents logged into a particular skill group that can be used for outbound dialing. For example, if there are 100 agents logged into skill group N, and the Outbound Percent variable is set to 50%, 50 agents would be allocated for outbound dialing.

**Note:** This variable does not allocate specific agents for outbound dialing, just a total percentage.

Use the Internet Script Editor application to create an administrative script for each Outbound Option skill group to control the Outbound Control variable and the skill group reservation percentage. The Outbound Option Dialer looks at the value of this variable to determine which mode each skill group uses.
Chapter 10

Installing and Configuring Cisco Multichannel Components for IPCC Enterprise

This section describes how to install and configure Cisco Multichannel software for IPCC Enterprise.

This section contains the following topics:

• About IPCC Enterprise Multichannel Components, page 91
• About Multichannel Installation Prerequisites, page 92
• How to Install Multichannel Components for IPCC Enterprise, page 92
• About IPCC Configuration for Multichannel Components, page 93
• How to Configure Multichannel Components for IPCC Enterprise, page 97

About IPCC Enterprise Multichannel Components

IPCC Multichannel components include the Cisco Collaboration Server and Cisco E-Mail Manager. These optional IPCC components provide Web and E-mail interactivity to IPCC.

About Cisco Collaboration Server

Cisco Collaboration Server (CCS) provides Web collaboration between a caller and contact center agent. Agents can share information with customers over the Web, such as Web pages, forms, and applications, while at the same time conducting a voice conversation or a text chat. Collaboration Server routes requests to the Central Controller via a Multichannel Controller, and the Central Controller then selects the agent to handle the request.

When deployed with IPCC Enterprise, CCS must be deployed with Cisco Media Blender. Cisco Media Blender (CMB) functions as an event bus, sharing software events between Collaboration Server and IPCC. It provides a firewall gateway to allow communication between the
Collaboration Server, which resides outside the firewall, and the Multichannel Controller inside the firewall. CMB must be installed on the Multichannel Controller for Collaboration Server.

About Cisco E-Mail Manager

Cisco E-Mail Manager (CEM) manages high volumes of customer inquiries submitted to company e-mail boxes or a Web site. E-Mail Manager selects agents and teams to receive incoming messages, categorizes and prioritizes messages, suggests response templates, and, if desired, sends automatic responses. E-Mail Manager sends route requests to the Central Controller via a Multichannel Controller, and the Central Controller routes the request to an available agent. The CEM T Server software must be installed on the Multichannel Controller for E-Mail Manager.

About Multichannel Installation Prerequisites

Before installing and configuring multichannel applications for use with IPCC Enterprise, you must:

<table>
<thead>
<tr>
<th>Installation Prerequisite</th>
<th>Installation Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install and configure the IPCC Central Controller, Agent/IVR Controller, and Administration &amp; WebView Reporting components.</td>
<td></td>
</tr>
<tr>
<td>Install and configure one Multichannel Controller for each multichannel option being deployed.</td>
<td></td>
</tr>
</tbody>
</table>

How to Install Multichannel Components for IPCC Enterprise

Step-by-step installation instructions for Multichannel components are included in the guides listed below. There are no IPCC-specific installation instructions for Multichannel components.

- Cisco Collaboration Server Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions
- Cisco Media Blender Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions
- Cisco E-Mail Manager Installation and Configuration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions
About IPCC Configuration for Multichannel Components

Before configuring IPCC for Multichannel options, you must understand these concepts described in this section:

• About Multichannel Controllers
• Media Routing Domains and Media Classes
• Multichannel Agents
• Application Instances (Multichannel Authentication)
• About Administration Connections
• Multichannel Skill Groups
• Universal Queue and Multichannel Routing Scripts

About Multichannel Controllers

To route any Multichannel request, you must establish a Multichannel Controller. The Multichannel Controller accepts and translates information in requests initiated from the Web or through E-Mail into information that IPCC routing scripts can understand.

When IPCC receives a new task request from the application, it runs a pre-defined IPCC script to determine how to handle the task. As a result of the execution of the script, IPCC sends an instruction to the application to do one of the following:

• Execute an application script that is stored on the application server, and return the application script execution result to IPCC. IPCC then tries to find a best available agent that has the matching skill within the enterprise, and assigns this agent to this task.

• Handle the new task with an IPCC-determined best available agent that has the matching skill within the enterprise.

Note: You can use IPCC Web Collaboration software to route Web Callback and Delayed Callback requests.

About Media Routing Domains

IPCC uses Media Routing Domains (MRDs) to organize how requests for different media are routed. An MRD is a collection of skill groups that are associated with a common communication medium. IPCC uses an MRD to route a task to an agent who is associated with a skill group and a particular medium.
System IPCC supports five classes of Media Routing Domains:

- Multi-session chat
- Single-session chat
- Blended Collaboration
- Voice (used for traditional voice calls, as well as Web Callback and delayed callback, and Blended Collaboration using legacy ACDs)
- E-Mail

About Multichannel Agents

In an IPCC configuration, you can create two different types of agents:

- Voice agents--Agents who can receive telephone calls are referred to as Voice agents. Note that a Voice agent can also be configured to receive non-voice requests, such as Single-session Chat, Multi-Session Chat, and E-Mail.
- Non-voice agents--Agents who can receive only non-voice requests. That is, non-voice agents cannot use the phone

You can create agents using either the IPCC Web Configuration Tool or the administration interface for the multichannel software you're deploying. However, in order to use multichannel applications, agents must A) be enabled those for multichannel applications, and B) be assigned multichannel skill groups. This can only be done in the administration interface for the multichannel software you're deploying.

Configuring an agent for multichannel means assigning that agent to at least two skill groups (one for each media). For example, the agent might handle both e-mail and phones, Single-session chat and phones, or Blended Collaboration and e-mail.

In most cases, the Agent/IVR Controller tracks and records the state and activity of all voice and non-voice agents.

See Also

Cisco Collaboration Server Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions
Cisco Web Collaboration Administration online help
Cisco E-Mail Manager Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions
Cisco E-Mail Manager Administration online help

About Multichannel Skill Groups

In a Multichannel configuration, skill groups are medium-specific. When an agent logs in via phone, or Web Collaboration, or E-Mail Manager, the agent automatically logs into skill groups.
associated with that agent within the correct MRD. Then, as a task request for a specific MRD begins script execution, the Agent/IVR Controller considers only the skill groups associated with that specific MRD. This allows one script to be written to handle many MRDs.

You can use the IPCC Web Administration Tool to create and view skill groups for the Voice MRD only. You must create and manage skill groups for Multi-session chat, Single-session chat, Blended Collaboration, and E-Mail using the Multichannel software options.

The following table outlines the proper procedures for creating skill groups:

<table>
<thead>
<tr>
<th>Create skill groups for this Media Class...</th>
<th>...using the interface for this software:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>IPCC Web Administration Tool</td>
</tr>
<tr>
<td>Multi-session chat, Single-session chat, Blended Collaboration</td>
<td>IPCC Web Collaboration option (CCS)</td>
</tr>
<tr>
<td>E-Mail</td>
<td>IPCC E-Mail Manager option (CEM)</td>
</tr>
</tbody>
</table>

About Application Instances (Multichannel Authentication)

An application instance represents a single software application that has been integrated with IPCC. System IPCC supports a single application instance each for Collaboration server and E-Mail Manager. These instances must be configured in IPCC.

You configure multichannel authentication through the Multichannel Authentication page in the IPCC Web Administration Tool. For each Multichannel option that you want to use, you must establish an application key (password) that identifies the multi-media feature you want to implement. Once you have configured multichannel authentication in IPCC, you must also create matching application instances in Collaboration Server and E-Mail Manager.

Use the form below to make note of the application instance and key you assign to each feature. You can use the information here later when you establish the Application Instance on ICM, Collaboration, and E-Mail software.

<table>
<thead>
<tr>
<th>Configuration element</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application instance ID for Collaboration</td>
<td>CCS (hard-coded)</td>
</tr>
<tr>
<td>Application key for Collaboration</td>
<td>cisco (default)</td>
</tr>
<tr>
<td>Application instance for E-Mail</td>
<td>CEM (hard-coded)</td>
</tr>
<tr>
<td>Application key for E-Mail</td>
<td>cisco (default)</td>
</tr>
</tbody>
</table>

About Administration Connections

You must configure a communications path between IPCC and the multichannel software.
Connections between the multichannel software and IPCC Administration & WebView Reporting use Java Remote Method Invocation (RMI). With such a connection, an RMI registry exists on both sides of the firewall. Each registry identifies its machine to the machine on the other side of the firewall.

When configuring IPCC and Multichannel options, note that each connection registers at its registry port using its link name. You must therefore define a link name and a registry port for IPCC Administration & WebView Reporting, the Collaboration server, and the E-Mail Manager server.

Before you begin, gather the information in the table below.

<table>
<thead>
<tr>
<th>Configuration element</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name or IP address of the IPCC Administration &amp; WebView Reporting Machine</td>
<td></td>
</tr>
<tr>
<td>IPCC Administration &amp; WebView Reporting service name</td>
<td></td>
</tr>
<tr>
<td>IPCC Administration &amp; WebView Reporting RMI registry port</td>
<td></td>
</tr>
<tr>
<td>Host name or IP address of the Collaboration server</td>
<td></td>
</tr>
<tr>
<td>Application service name for the Collaboration server</td>
<td></td>
</tr>
<tr>
<td>RMI registry port for the Collaboration server</td>
<td></td>
</tr>
<tr>
<td>Host name or IP address of the E-Mail Manager server</td>
<td></td>
</tr>
<tr>
<td>Application service name for the E-Mail Manager server</td>
<td></td>
</tr>
<tr>
<td>RMI registry port for the E-Mail software</td>
<td></td>
</tr>
</tbody>
</table>

About Universal Queue and Multichannel Routing Scripts

Universal Queue is a feature of the IPCC architecture that places multiple media types under the routing control of IPCC. IPCC routing scripts allow you to target a task to a specific agent. The Queue to Agent Script node enables an agent to receive and work more than one task at a time. As a result, Universal Queue coordinates an agent's ability to work on multiple tasks of various media. It supports a simple control model where an agent's ability to handle an additional task depends on what task that agent is currently handling. For this level of control, IPCC must have exclusive access to task assignment.

The Queue to Agent node allows the targeting of a task (the work performed by an agent) to a script-specified agent. For Universal Queue to work, the agent must be assigned to skill groups where IPCC picks the agent. (IPCC automatically picks the agent for Voice skill groups.)
The Central Controller has the ability to move tasks out of the present script execution and resubmit them into the system as a new invocation.

How to Configure Multichannel Components for IPCC Enterprise

After installation, Multichannel components must be configured for integration with IPCC.

The following table lists the configuration tasks required for Multichannel components in an IPCC Enterprise deployment. Perform tasks in the order listed. Instructions for each are included later in this section.

<table>
<thead>
<tr>
<th>Configuration Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optionally, modify Media Routing Domain configuration</td>
<td></td>
</tr>
<tr>
<td>Configure application key for multichannel authentication</td>
<td></td>
</tr>
<tr>
<td>Establish administration connections</td>
<td></td>
</tr>
<tr>
<td>Set call variables</td>
<td></td>
</tr>
<tr>
<td>Write IPCC routing scripts for multichannel options</td>
<td></td>
</tr>
<tr>
<td>Configure Cisco Web Collaboration Server for IPCC integration</td>
<td></td>
</tr>
<tr>
<td>Configure Cisco Media Blender for IPCC integration</td>
<td></td>
</tr>
<tr>
<td>Configure Cisco E-Mail Manager for IPCC integration</td>
<td></td>
</tr>
</tbody>
</table>

How to Modify Media Routing Domain Configuration

A Media Routing Domain for each supported media class is created and configured automatically by IPCC during installation. These can be used as is; or, if desired, you can modify the default settings for any of the MRDs you are deploying.
The Media Routing Domains supported by System IPCC are:

- Multi-session chat
- Single-session chat
- Blended Collaboration
- E-Mail
- Voice

To modify the default settings for MRDs you are deploying:

**Step 1** In the IPCC Web Administration Tool, select Multichannel Management > Media Routing Domains.

**Step 2** Click the MRD you want to modify.

**Step 3** Modify default values as desired. Consult the online Help for the Media Routing Domains page for instructions on completing individual fields.

How to Configure Application Instances

An application instance for each multichannel option is created and configured automatically by IPCC during installation. While these can be used as is, in most cases you may prefer to modify the default password created at installation.

To configure application instances:

**Step 1** In the IPCC Web Administration Tool, select Multichannel Management > Multichannel Authentication.

**Step 2** On the Multichannel Authentication list page, click the multi-channel application (CCS or CEM) you want to edit.

**Step 3** Under Application Key, select Change.

**Note:** Record the application key. You need to enter this value in your multichannel applications.

**Step 4** Enter and re-enter the Application Key. This is the password that the integrated application will use to be identified by IPCC.

**Step 5** Click Save.

**Step 6** Repeat this procedure to add the application instance for the other application type.
How to Establish Administration Connections

You must configure a communications path between IPCC and the Multichannel software.

You must ensure that values entered on the IPCC Administration & WebView Reporting machine match those entered on the Collaboration Server and E-Mail software.

Perform the following steps for each multi-media server you are setting up. For instance, if you are setting up two servers--for Collaboration and one for E-Mail--you must set up two separate administration connections.

To establish administration connections:

**Step 1** From the IPCC Administration program group on the IPCC Administration & WebView Reporting machine, select CMS Control.

**Step 2** Select the Application tab.

**Step 3** Click Add. The Application Connection Details dialog box displays.

**Step 4** Enter the application connection properties as follows:

ICM Distributor AW link. Enter the link name on the IPCC software. This can be any value, but must match the value you configure for “remote link name” in your multichannel applications.

ICM Distributor AW RMI registry port. Enter the RMI registry port number you want the IPCC Administration & WebView Reporting machine to use.

**Note:** To prevent conflicts with SQLServer which will use port 1099 under certain circumstances, Cisco recommends that you use port number 2099 rather than the default.

Application link. Enter the link name for the Collaboration or E-Mail server.

Application RMI registry port. Enter the RMI registry port number you want the Collaboration or E-Mail server to use. All multichannel applications must use the same ports, and this value must match the port number you entered for the ICM Distributor AW RMI registry port.

**Note:** To prevent conflicts with SQLServer which will use port 1099 under certain circumstances, Cisco recommends that you use port number 2099 rather than the default.

Application host name. Enter the host name or IP address of the Collaboration server or E-Mail server.

**Step 5** Click OK twice. This restarts the Cms_Jserver on the Administration & WebView Reporting machine.
How to Set Call Variables

Several call variables must be configured in the IPCC Web Administration Tool--for each integrated multichannel feature--in order to route multichannel requests.

Three call variables are automatically installed for the E-Mail software. These are:

- cisco.CEM.Category
- cisco.CEM.MessageKey
- cisco.CEM.Priority

You must set up two variables if you intend to use the Blended Collaboration and/or Voice Media Routing Domains (to route Web or Delayed Callback requests). The ECC variables are:

- user.cisco.cmb
- user.cisco.cmb.callclass

Use the Call Variables page in the IPCC Web Administration Tool to limit the user.cisco.cmb variable to 8 bytes and the user.cisco.cmb.callclass variable to 10 bytes to prevent call variable space limitations.

**Note:** You need not specify these variables in your input map on the Collaboration server. These variables are added to your input map whenever you enable the Voice or Blended Collaboration MRDs.

In addition, if changes are made to the call variables in your inmap file, or to call variables in IPCC, you must restart Cisco Collaboration Server for changes to take effect.

To configure call variables, complete these steps:

**Step 1**
In the IPCC Web Administration Tool, select Contact Management > Call Variables.

**Step 2**
Click Create.

**Step 3**
Complete the required data.

**Step 4**
Click Save.
How to Write IPCC Routing Scripts for Multichannel Options

You must also write routing scripts that will route Multichannel requests to appropriate agents.

Once you have completed the Collaboration Server and/or E-Mail Manager set up, write scripts to test routing of each media, and universal queue. See the *ICM Scripting and Media Routing Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* and your multichannel documentation for instructions on creating routing scripts for multichannel applications.

How to Configure Cisco Collaboration Server for IPCC Integration

Setting up Collaboration software to suit your contact center's needs involves many steps. The following checklist outlines those steps that pertain to setting up the integration with IPCC software.

**Note:** If you are deploying the Cisco Dynamic Content Adapter with Collaboration Server, you do not need to perform any IPCC-specific tasks to integrate with IPCC. Configure DCA as described in the Cisco Dynamic Content Adapter documentation set.

To configure Collaboration Server for IPCC integration:

1. **Step 1** Identify the Collaboration Server machine.
2. **Step 2** Run the Integrate with ICM wizard. This wizard walks you through defining the CCS application instance in an IPCC-integrated configuration and establishing an IPCC Administration connection to IPCC Administration & WebView Reporting.

   The wizard also covers:

   - **Enabling IPCC Media Routing Domains**
   - **Establishing Media Blender connections.** When you perform this step, you must copy two files from the Collaboration machine to the Media Blender machine. These files are `<connection>.properties` and `collaboration.properties`.

   - **Enabling IPCC Agent Peripheral.** You must enable the peripheral that will track agent activity. This is the IPCC Agent/IVR Controller.

3. **Step 3** Create queues.
4. **Step 4** Create agents and skill groups.
5. **Step 5** Configure HTML callforms to gather caller information.
How to Configure Cisco Media Blender for IPCC Integration

To configure Media Blender for IPCC integration:

**Step 1** Configure the ciscocti.properties file.

**Step 2** Configure the firewall gateway.

See Also

*Cisco Media Blender Installation Guide*
*Cisco Media Blender Administration Guide*

How to Configure Cisco E-Mail Manager for IPCC Integration

Setting up E-Mail software to suit your contact center's needs involves many steps. The following list outlines those steps that pertain to setting up the integration with IPCC.

**Note:** In the steps below, if you are using two IPCC Administration & WebView Reporting machines, either machine can be specified.

To configure E-Mail Manager for IPCC integration:

**Step 1** Complete the ICM Tab in the E-Mail Manager configuration utility. You must enter the following information on this tab:

- The E-Mail Manager application instance name (CEM) and application key
- The IPCC Media Routing Domain
- The Administration Connection name to the IPCC Administration & WebView Reporting machine
- RMI Service Name and Registry port for E-Mail Manager software
- RMI Service Name and Registry port for the IPCC Administration & WebView Reporting machine
- Host Name of the IPCC Administration & WebView Reporting machine
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Establish an Administration connection to the Administration &amp; WebView Reporting machine.</td>
</tr>
<tr>
<td>3</td>
<td>Enable ICM Media Routing Domains.</td>
</tr>
<tr>
<td>4</td>
<td>Enable IPCC Agent Peripheral--You must enable the peripheral that will track agent activity. This is the IPCC Agent/IVR Controller.</td>
</tr>
<tr>
<td>5</td>
<td>Configure ICM Routing skill groups and agents.</td>
</tr>
<tr>
<td>6</td>
<td>Configure rules to route messages to those skill groups.</td>
</tr>
</tbody>
</table>

**See Also**

- Cisco E-Mail Manager Installation and Configuration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions
- Cisco E-Mail Manager Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions
- Cisco ICM E-Mail Manager: Administration online help
Chapter 11

Configuring Reporting for IPCC Enterprise

This section describes tasks required to configure reporting for your IPCC Enterprise system. Refer to the Reporting Guide for Cisco IPCC Enterprise & Hosted Editions for important IPCC Enterprise reporting conceptual information and planning considerations.

Most of the setup required for IPCC Enterprise reporting is accomplished in the course of normal IPCC component configuration described elsewhere in this document. This section consolidates that information, and lists additional required and optional reporting configuration tasks beyond those covered earlier. The tasks described in this section are all performed using the IPCC Web Administration Tool.

This section contains the following topics:

- About Reporting Configuration Prerequisites, page 105
- IPCC Reporting Configuration Tasks, page 106
- How to Configure Service Levels, page 106
- How to Configure Bucket Intervals, page 108
- How to Configure Short Calls, page 109
- About Other Reporting Setup Options, page 110

About Reporting Configuration Prerequisites

Before performing the reporting configuration tasks in this section, you must:

1. Install and configure Call Manager
2. Install and configure IP IVR
3. Install and configure the Central Controller, Agent/IVR Controller, and Administration & Reporting
4. Create Call Types, agents and Skill Groups.
IPCC Reporting Configuration Tasks

Below are the basic reporting configuration tasks required in an IPCC Enterprise system. Perform tasks in the order listed. Instructions for each are included later in this section.

1. Configure Service Levels for Call Types and Skill Groups
2. Configure Bucket Levels
3. Optionally, modify Short Calls configuration
4. Optionally, modify other features that affect reporting

How to Configure Service Levels

Service Level configuration allows you set and measure goals for answering calls. For example, your goal might be to answer 80% of calls within two minutes. By configuring Service Level settings accordingly, your reports can then show you the percentage of calls that are answered within that time threshold. In Service Level configuration, you also determine how abandoned calls should impact the Service Level.

You define Service Level settings for Call Types and Skill Groups. Global Service Level settings must be defined for each. These can be overridden by local settings for specific Call Types and Skill Groups.

For Call Types, global Service Level settings are specified in Call Type Global Options. The system-default values for global Call Type Service Level are:

- Call Type Service Level Threshold: 20
- Call Type Service Level Type: Ignore abandoned calls

For Skill Groups, global Service Level settings are specified as an attribute of each media routing domain to which your Skill Groups belong. The system-default global Service Level values for all MRDs are:

- Skill Group Service Level Threshold: 30
- Skill Group Service Level Type: Ignore abandoned calls

How to Modify the Global Service Level for Call Types

To modify the global Call Type Service Level for your IPCC Enterprise system:
### How to Configure Service Levels

| Step 1 | In the IPCC Web Administration Tool, select Call Management > Call Types > Global Options. |
| Step 2 | Specify a value for Service Level Threshold, in seconds. |
| Step 3 | Select the Service Level Type. |
| Step 4 | Click Save. |

### How to Set Service Levels for Specific Call Types

If desired, you can also configure the Service Levels for specific Call Types. These will override the system level setting:

| Step 1 | In the IPCC Web Administration Tool, select Contact Management > Call Types. |
| Step 2 | Select the Call Type whose Service Level you want to set. |
| Step 3 | Set Service Level Threshold to Use Specified Threshold. |
| Step 4 | Specify a value for Service Level Threshold, in seconds. |
| Step 5 | Select the Service Level Type. |
| Step 6 | Click Save. |

### How to Modify the Global Service Level for Skill Groups

To modify the global Skill Group Service Level for your IPCC Enterprise system:

| Step 1 | In the IPCC Web Administration Tool, select Multichannel Management > Media Routing Domains. |
| Step 2 | Select the media routing domain you want to work with. |
| Step 3 | Specify a value for Service Level Threshold, in seconds. |
| Step 4 | Click Save. |

**Note:** The global Service Level Type setting for Skill Groups is Ignore Abandoned Calls. This setting is not editable at the global level and is not visible in the IPCC Web Administration Tool interface.
How to Set Service Levels for Specific Skill Groups

If desired, you can also configure the Service Levels for specific Skill Groups. These will override the system level setting on the media routing domain:

**Step 1** In the IPCC Web Administration Tool, select Contact Management > Skill Groups.

**Step 2** Select the Skill Groups whose Service Level you want to set.

**Step 3** Set Service Level Threshold to Use Specified Threshold.

**Step 4** Specify a value for Service Level Threshold, in seconds.

**Step 5** Select the Service Level Type.

**Step 6** Click Save.

How to Configure Bucket Intervals

Bucket Intervals allow you to track data for calls abandoned or answered within specific time increments (for example, between 0 and 8 seconds, or under 60 seconds). Bucket Intervals are associated with Call Types and can be set for the system as a whole and for individual Call Types. Local settings override those set at the system level. By configuring intervals in relation to your Service Levels, you can track how closely to your Service Level calls are abandoned. You can create multiple Bucket Interval groups for use with different Call Types.

To avoid reporting inconsistencies, only modify Bucket Interval settings at specific time boundaries (that is, end of day, week, or month). Ensure that no one is running reports for the intervals that you are changing when you modify the boundaries.

IPCC ships with a single system default Buckets Interval whose boundaries (increments) are: 8, 30, 60, 90, 120, 180, 300, 600, and 1200 (in seconds).

How to Create Bucket Intervals

Before you can assign a Bucket Interval (either as the new global default or to a particular Call Type) you must create its definition. To define a Bucket Interval:

**Step 1** In the IPCC Web Administration Tool, select Call Management > Advanced > Bucket Intervals.

**Step 2** Click Create.

**Step 3** In the Add Name field, enter a name for the interval.

**Step 4** In the Upper Bounds fields, add up to nine successive increments to measure, in seconds.
How to Re-Set the Global Bucket Interval

To re-set the Global Bucket Interval for your IPCC Enterprise system:

Step 1 In the IPCC Web Administration Tool, select Call Management > Call Types > Global Options.
Step 2 In the ICM Configuration Manager, select Tools > Miscellaneous Tools > System Information.
Step 3 Click Save.

How to Set Bucket Intervals for Specific Call Types

If desired, you can also configure Bucket Intervals for specific Call Types. These will override the global level setting:

Step 1 In the IPCC Web Administration Tool, select Contact Management > Call Types.
Step 2 Select the Call Type whose Bucket Interval you want to set.
Step 3 From the Bucket Intervals list, select the interval you want to use.
Step 4 Click Save.

How to Configure Short Calls

A Short Call is a call that is either abandoned or answered very quickly. By defining what you believe to be a short call, then you can filter out those calls that you believe did not stay in the system long enough to be counted as a real call. Short Calls are configured for Call Types only, and only at the global level, meaning you cannot create different short call definitions for specific Call Types. The system default is 5 seconds.

Note: The concept of Short Calls applies to the Voice media class only.

How to Configure Short Calls for Call Types

To configure Abandoned Short Calls for Call Types:

Step 1 In the IPCC Web Administration Tool, select Contact Management > Call Types > Global Options.
Step 2  Set Abandoned Call Wait Time to a value, in seconds. This value indicates the length of calls to be considered abandoned. Calls that last longer than this are not considered abandoned. To not track abandoned calls, leave the field blank.

Step 3  Click Save.

About Other Reporting Setup Options

This section lists additional IPCC Enterprise features whose configuration has reporting implications.

About IPCC Supervisory Features

Supervisors of agent teams can take advantage of supervisory features available with their Agent Desktop software.

Supervisory features include:

• Supervisor and emergency assist: Allows agents to activate supervisor assist or emergency assist buttons on their desktop.

• Barge-In: Allows a supervisor to conference into an agent call from his or her desktop.

• Intercept: Allows a supervisor to intercept (take over) a call from his or her desktop.

Note: These supervisory features apply only to IPCC voice contact. They are not available to agents using Media Routing Domains (MRDs) other than Voice.

The IP Contact Center Enterprise Edition Reporting Guide provides guidelines and details for setting up supervisory features.

About Agent Transfer and Conferencing

Agents can transfer or conference a call by manually transferring the call to another agent or by conferencing-in another agent or party by dialing the recipient's extension directly.

The IP Contact Center Enterprise Edition Reporting Guide provides guidelines and details for setting up agent transfer and conferencing.

See Also

Cisco IP Contact Center Enterprise Edition Administrator Guide
Cisco IP Contact Center Enterprise Edition Reporting Guide
Part 3: Appendixes
Chapter 12

IPCC Troubleshooting

This section contains the following topics:

- Installation Issues, page 113
- Machine Initializer and Active Directory Issues, page 114
- Tomcat and IIS Issues, page 115
- IPCC Web Administration Access Errors, page 116
- Machine Creation/Modification Errors, page 117
- Write to Database Issues, page 118
- Database Connection Issues, page 119
- Miscellaneous Issues/Information, page 120

Installation Issues

This section offers workarounds for issues that can occur during installation of the IPCC controllers and Administration & WebView Reporting machines.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Condition</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installer complains SQLServer missing or insufficient service pack</td>
<td>Occurs if SQLServer2000 has not been installed on a machine on which the Central Controller and/or Administration &amp; WebView Reporting is being installed.</td>
<td>1. Stop installer. 2. Install SQLServer 2000 using setting specified in the Staging Guide for ICM/IPCC Enterprise and Hosted Editions. 3. Apply appropriate SQLServer service pack as specified in the Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials. 4. When complete, restart installer.</td>
</tr>
<tr>
<td>Installer complains SQLServer protocols in wrong order</td>
<td>Occurs if TCP IP protocol is ordered before Named Pipe in SQLServer configuration.</td>
<td>1. Stop installer. 2. Reorder protocols via Start &gt; Programs &gt; MS SQL Server &gt;Client Network Utility. 3. When complete, restart installer.</td>
</tr>
</tbody>
</table>
Machine Initializer and Active Directory Issues

This section offers workarounds for issues pertaining to the IPCC Machine Initializer and/or Active Directory.

### Symptom | Condition | Workaround
--- | --- | ---
Installer complains SNMP or WMI not detected | Occurs if Windows SNMP Services not fully installed | Stop installer and install SNMP/WMI as described below (Note: you may need to have the Windows OS install media to complete this operation):
2. Select Management and Monitoring Tools check box.
3. Click Details button.
4. Select the SNMP and WMI check boxes.
5. Click OK/Next to complete the Add Windows Components wizard. When complete, resume install.
Note: SNMP/WMI is only needed for CDP, an optional monitoring feature of IPCC. If you do not plan to use CDP, you can ignore the error message during the install.

Installer complains a service could not be started because it is already running | Occurs if one or more services the installer attempts to start is already running. | Message can be safely ignored. If you get one of these errors, the installer will allow you to Retry or Cancel. It is OK to Cancel.

### Machine Initializer and Active Directory Issues

This section offers workarounds for issues pertaining to the IPCC Machine Initializer and/or Active Directory.

### Symptom | Condition | Workaround
--- | --- | ---
Machine Initializer returns “…cannot bind to GUID…” error. | Occurs if machine cannot connect to the domain controller. | Run netdiag from Windows 2003 support tools. Verify your computer is in the domain and its DNS server can locate the Domain Controller. Verify the Domain Controller is up and running.

Cannot create a Cisco_ICM Root or Facility | Occurs if you do not have the necessary Active Directory privileges. | Make sure you are running with the correct permissions Run netdiag from Windows 2003 support tools

Error returned by IPCC Machine Initializer | The domain controller is not in native mode. | Consult your Domain Administrator.
The Machine Initializer Log files are located at: c:\temp\ipccMachineInitialization.log. When launched, by the IPCC Installer, Machine Initializer tracing and error messages appear in the installation log file located at: c:\temp\IPCCInstallLogs\<date_stamp>\IPCCInstall.log.

See the Staging Guide for ICM/IPCC Enterprise and Hosted Editions for additional Active Directory troubleshooting instructions.

**Tomcat and IIS Issues**

Tomcat and IIS are required to serve IPCC Web-based applications including the IPCC Web Administration Tool, WebView, and the Agent Re-skilling Tool.

IPCC Web Administration uses Tomcat as its servlet engine. Tomcat is installed to icm\tomcat and runs as a service--Apache Tomcat. The Tomcat service startup type is set to as Automatic and the service starts automatically after installation. It runs as a domain user with local administrator rights for JDBC access, remote registry, and services access. Access to Tomcat is allowed only through SSL and the IIS front-end. Direct access to Tomcat ports is disabled during installation.

Tomcat log files are located at: icm\tomcat\logs. Additional IPCC Web Administration log files are located at: icm\tomcat\webapp\uiroot\WEB-INF\logs. There are both error and trace log files.

As necessary, to troubleshoot Tomcat issues, turn up logging by modifying the value for the APIServer.TraceFilter.sysTraceFilter.verbosity property in this file: icm\tomcat\webapps\uiroot\WEB-INF\properties\common\apiserver\logManager\APIServer.properties. The default, value is VERBOSITY_NONE (logging is off). To turn logging up, change the value the LOCAL_DUMP then restart the Tomcat service.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Condition</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tomcat service does not start.</td>
<td>Check the Windows Services panel and Tomcat log files for errors.</td>
<td></td>
</tr>
<tr>
<td>Tomcat starts up but cannot load sadlib.dll</td>
<td>Tomcat service path is incorrect.</td>
<td>Verify icm\bin is specified as the path to the service executable.</td>
</tr>
<tr>
<td>Pages served via Tomcat render slowly.</td>
<td>Usually occurs the first time Tomcat must render a page.</td>
<td>Self-correcting; Pages will render more quickly on subsequent access.</td>
</tr>
</tbody>
</table>
Microsoft Internet Information Service (IIS) is used as the front-end to Tomcat. It uses Apache ISAPI dll to connect to Tomcat icm\tomcat\bin\i386\isapi_redirector2.dll. If you suspect issues related to IIS, ensure that:

- The IIS Virtual Directory points to the directory: icm\tomcat\bin\i386
- IIS manages the SSL layer. SSL is enabled by default during IPCC installation with a self-signed certificate. Both “Require Secure channel (SSL)” and “Require 128-bit encryption” must be set.
- In IIS 6, Web Services Extensions lists jakarta as Allowed.

**IPCC Web Administration Access Errors**

This section offers workarounds for issues that can occur accessing the IPCC Web Administration Tool.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Condition</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot access the IPCC Web Administration Tool...browser returns page not found error</td>
<td>Tomcat service is not started on Administration &amp; WebView Reporting machine...OR...IIS is not started on Administration &amp; WebView Reporting machine</td>
<td>Start the Apache Tomcat service and/or IIS via Windows Services panel.</td>
</tr>
<tr>
<td>Cannot access the IPCC Web Administration Tool...URL is accessible but UI fails to display</td>
<td>Occurs in Internet Explorer running on Windows 2003, the result of IE's Enhanced Security Configuration, standard on Windows 2003.</td>
<td>1. Access the IPCC Web Administration Tool from a browser on another machine not running Windows 2003...OR...2. In the 2003 browser, select Tools &gt; Internet Options &gt; Security. Selected Trusted Sites &gt; Sites and add your URL to the list of trusted sites. Note that you may have to reboot the machine to get the trusted site to work...OR...3. Turn off IE Enhanced Security Configuration for the machine via Start &gt; Control Panel &gt; Add/Remove Programs &gt; Add/Remove Windows Components &gt; Internet Explorer Enhanced Security Configuration. Then restart the browser.</td>
</tr>
<tr>
<td>Can't login via login page</td>
<td>You are not using valid AD username/password or don't belong to proper AD Security Group...OR...the Domain Controller is down...OR...the connection between the Domain Controller and the Administration &amp; WebView Reporting machine is down.</td>
<td>Verify you are using valid AD username/password and belong to the proper AD Security Group...OR...verify the Domain Controller is up...OR...verify the network connection to the Domain Controller is up. As a last resort, re-start the Administration &amp; WebView Reporting machine.</td>
</tr>
</tbody>
</table>
### Machine Creation/Modification Errors

This section offers workarounds for some that can occur when creating or modifying machines in the IPCC Web Administration Tool.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Condition</th>
<th>Workaround</th>
</tr>
</thead>
</table>
| IPCC Web Administration Tool forces you to accept a certificate each time you access it. | Occurs when you access the IPCC Web Administration Tool Login page. | 1. Install the certificate as follows: a) In the IE Security Alert dialog, click View Certificate; b) Click Install Certificate, then follow prompts to complete the installation.  
2. In the 2003 browser, select Tools > Internet Options > Security. Selected Trusted Sites > Sites and add your URL to the list of trusted sites. Note that you may have to reboot the machine to get the trusted site to work.  
OR...2. In the 2003 browser, select Tools > Internet Options > Security. Selected Trusted Sites > Sites and add your URL to the list of trusted sites. Note that you may have to reboot the machine to get the trusted site to work...OR...3. Turn off IE Enhanced Security Configuration for the machine via Start > Control Panel > Add/Remove Programs > Add/Remove Windows Components > Internet Explorer Enhanced Security Configuration. Then restart the browser.  
OR...2. In the 2003 browser, select Tools > Internet Options > Security. Selected Trusted Sites > Sites and add your URL to the list of trusted sites. Note that you may have to reboot the machine to get the trusted site to work...OR...3. Turn off IE Enhanced Security Configuration for the machine via Start > Control Panel > Add/Remove Programs > Add/Remove Windows Components > Internet Explorer Enhanced Security Configuration. Then restart the browser.  
OR...2. In the 2003 browser, select Tools > Internet Options > Security. Selected Trusted Sites > Sites and add your URL to the list of trusted sites. Note that you may have to reboot the machine to get the trusted site to work...OR...3. Turn off IE Enhanced Security Configuration for the machine via Start > Control Panel > Add/Remove Programs > Add/Remove Windows Components > Internet Explorer Enhanced Security Configuration. Then restart the browser. |
| IPCC Web Administration Tool functionality seems to be missing or incomplete. | You are using an unsupported browser...OR...popup blocking is enabled on your browser...OR...javascript is not enabled on your browser. | Consult the ICM/IPCC Bill of Materials (BOM) for supported browser versions...OR...disable popup blocking...OR...enable javascript for your browser. |

### Machine Creation/Modification Errors

This section offers workarounds for some that can occur when creating or modifying machines in the IPCC Web Administration Tool.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Condition</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IPCC Web Administration Tool returns an &quot;unable to find registry&quot; error when you attempt to create or modify a machine.</td>
<td>The machine Hostname or IP Address is incorrect...OR...the machine is not running...OR...IPCC has not been installed correctly in the machine...OR...the IPCC Machine Initializer has not been run on the machine...OR...File and Printer Sharing for Microsoft Networks is not enabled on that machine.</td>
<td>Verify the machine Hostname or IP Address...OR...verify the machine is running...OR...verify IPCC has been installed correctly in the machine...OR...rerun the IPCC Machine Initializer on the machine...OR...enable &quot;File and Printer Sharing for Microsoft Networks&quot; at Start &gt; Settings &gt; Network Connections... Local Area Connections &gt; General tab &gt; Properties.</td>
</tr>
</tbody>
</table>
| The IPCC Web Administration Tool returns an "unable to start services" error when you attempt to create or modify a machine. | Any of the conditions described for "unable to find registry" error (above)...OR... IPCC is timing-out attempting to connect to the machine. | Use workarounds for "unable to find registry" error (above)...OR...  
Increase the timeout value by adding the following line to properties.xml:  

```
<PROPERTY name="machineWizServicesTimeout" value="180" />
```

### Work to Database Issues

This section offers workarounds for issues that can occur when writing or connecting to the IPCC database.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Condition</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IPCC Web Administration Tool returns a &quot;Unable to start the Conapi Connection on this Administration &amp; WebView Reporting machine&quot; error.</td>
<td>IPCC timing out trying to make a write connection to the database.</td>
<td>You can increase the timeout value by adding the following line to properties.xml.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;PROPERTY name=&quot;machineWizConapiTimeout&quot; value=&quot;360&quot; /&gt;</code></td>
</tr>
<tr>
<td>IPCC machines are created in the Web Administration Tool but later fail to display - it appears as if they do not exist or were deleted.</td>
<td>Can occur in a duplexed environment if machine data written to the Side A database was not replicated to the Side B database (for example, if the Central Controllers were mistakenly configured as Simplexed) AND the Side A db is brought down, causing System IPCC to look to the Side B db for data.</td>
<td>Run the Synchronize command in the ICMDBA utility on the Central Controller Side A machine to synchronize the Side A and B databases. To synchronize using ICMDBA:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the tree under the selected machine in the ICMDBA dialog: Servers &gt; &lt;MachineName&gt; &gt; Instances &gt; ipcc &gt; LoggerA. Select ipcc_sideA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. From the Data menu, click Synchronize... Make sure the Source Server and Database pulldowns display the Central Controller and database that contain the Machines data (usually the Side A Central Controller and database). Make sure the Destination Server and Database pulldowns display the Central Controller and database that do not contain the Machines data (usually the Side B Central Controller and database).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click the Synchronize button.</td>
</tr>
</tbody>
</table>

### Write to Database Issues

180 is the default value-- the number of seconds the software tries to start each service or set of services before timing out.

Properties.xml is located at `<install drive>:\icm\tomcat\webapps\uiroot\web-inf\properties\default\ipccAdmin`

**Condition**

- IPCC timing out trying to make a write connection to the database.

**Workaround**

- Run the Synchronize command in the ICMDBA utility on the Central Controller Side A machine to synchronize the Side A and B databases. To synchronize using ICMDBA:
  2. Expand the tree under the selected machine in the ICMDBA dialog: Servers > <MachineName> > Instances > ipcc > LoggerA. Select ipcc_sideA.
  3. From the Data menu, click Synchronize... Make sure the Source Server and Database pulldowns display the Central Controller and database that contain the Machines data (usually the Side A Central Controller and database). Make sure the Destination Server and Database pulldowns display the Central Controller and database that do not contain the Machines data (usually the Side B Central Controller and database).
  4. Click the Synchronize button.
### Database Connection Issues

**JDBC**

IPCC Web Administration uses JDBC to talk to the local database on Administration & WebView Reporting machines for read operations. JDBC uses domain authentication so Tomcat service must be running as authorized account; this account is created automatically by the IPCC Machine Initializer.

JDBC connection errors shows up in error and log files as: ERROR CRITICAL IPCCAdminErrors.6 DB_QUERY_CONNECT_FAILED

JDBC connection properties are defined in:
icm\tomcat\webapps\uifrot\WEB-INF\properties\default\ipccAdmin\client.properties. In this files, the following property values must appear (note that host name, user, password, and domain properties are commented out):

- JDBCDriver=net.sourceforge.jtds.jdbc.Driver
- JDBCUrlPrefix=jdbc:jtds:sqlserver://
- #JDBCHostname=host
- #JDBCUser=user
- #JDBCPassword=pass
- #JDBCDomain=domain
- JDBCICMInstance=ipcc

**ConAPI**

The Configuration Application Programming Interface (ConAPI) allows IPCC and multichannel options to share configuration information about agents and their related skill groups. ConAPI runs on Administration & WebView Reporting machines.

ConAPI requires a fully-working path from the Administration & WebView Reporting machine to the Central Controller. IPCC automatically creates a ConAPI connection for the IPCC Web Administration Tool in the CMS Control Console utility. It is normal for the ConAPI connection to be down until you run the IPCC Deployment Wizard.
ConAPI connection error shows up in error and log files as: ERROR CRITICAL IPCCAdminErrors.7 DB_UPDATE_CONNECT_FAILED

Miscellaneous Issues/Information

This section offers workarounds for miscellaneous issues and other general system information.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Condition</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to reference the IPCC System PG Peripheral ID</td>
<td>In certain deployment scenarios, an external system or option may need to know the IPCC System PG Peripheral ID in order to establish a connection with System IPCC. One example of this is when trying to establish a System IPCC as a child in an IPCC Gateway deployment.</td>
<td>The IPCC System PG Peripheral ID is always 1000.</td>
</tr>
</tbody>
</table>
Chapter 13

About System IPCC Enterprise Databases

This section contains the following topics:

- Overview of IPCC Databases, page 121
- About IPCC Data, page 123
- About the IPCC Central Database, page 124
- Administration & WebView Reporting Local Database, page 124
- About the Historical Database, page 125
- About the WebView Database, page 125
- About the Outbound Option Database, page 126
- Configuration Management Service (CMS), page 126
- Historical Data Administration, page 126

Overview of IPCC Databases

Depending on your deployment model, IPCC may use up to five separate databases to store configuration and call transaction data. All IPCC databases are created and sized automatically during installation. Initial sizing of databases is well in excess of system capacity needs, meaning you should never need to resize your IPCC databases.
The table below lists the databases (excluding multichannel) created and used by System IPCC Enterprise.

<table>
<thead>
<tr>
<th>Database</th>
<th>Stores</th>
<th>DB Name</th>
<th>Machine Location</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Database</td>
<td>All IPCC configuration, script, and call transaction data</td>
<td>ipcc_side&lt;A or B&gt;</td>
<td>Central Controller sides A and B</td>
<td>14 Gb</td>
</tr>
<tr>
<td>Administration &amp; WebView Reporting Local Database</td>
<td>Copies of the Central database configuration data and scripts</td>
<td>ipcc_awdb</td>
<td>Administration &amp; WebView Reporting</td>
<td>1.4 Gb</td>
</tr>
<tr>
<td>Historical Database</td>
<td>All IPCC historical data that has expired on the Central database.</td>
<td>ipcc_hds</td>
<td>Administration &amp; WebView Reporting</td>
<td>14 Gb</td>
</tr>
<tr>
<td>Note: All-in-One deployments do not include or support a Historical database. They DO support historical reporting from the Central Database.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WebView Database</td>
<td>WebView configuration data</td>
<td>wvdb</td>
<td>Administration &amp; WebView Reporting</td>
<td>100 Mb</td>
</tr>
<tr>
<td>Outbound Option Database</td>
<td>Outbound Option data</td>
<td>ipcc_baA</td>
<td>Central Controller side A only</td>
<td>1.4 Gb</td>
</tr>
<tr>
<td>Note: Only used if Outbound Option is deployed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Note:

• In duplexed deployments (deployments that include physical side A and side B machines), copies of side A machines are maintained on side B and automatically synchronized with their side A counterparts.

• The "up to five separate databases" total above does not include the additional databases created by multichannel options (if you include multichannel options in your deployment). See the Cisco Collaboration Server and Cisco E-Mail Manager documentation for more information on multichannel databases.

• For specific information on the tables of the IPCC databases, see the Database Schema Handbook for Cisco ICM/IPCC Enterprise & Hosted Editions.

About IPCC Data

IPCC handles three types of data:

• Configuration data is stored in the Central, Historical, and local databases.

• Historical data is stored in the Central and the Historical databases

• Real-time data is stored in the local database.

Configuration and Script Data

Configuration data describe your call center; for example, all of your agents, call types, and dialed numbers are part of the configuration data. Configuration data can also include data that has been imported from other systems, such as workforce scheduling data. In duplexed Central Controller systems, configuration data is kept duplexed on both Central databases. It is always re-synchronized when a Central Controller is restarted. Script data is also kept in both Central databases. Script data include all call routing and administrative scripts that IPCC uses in call routing.

Historical and Real-time Data

Historical data and Real-time data provide information about certain objects in the system such as skill groups and agents. Real-time data provide current information on these objects.

Historical data fall into four categories: five-minute snapshots, half-hour summaries, call detail records, and events. The five-minute tables contain snapshot data, which are values that are derived from real-time data. Snapshot data provides a view of contact center activity at a particular instant. Since the five-minute values change frequently, they are not synchronized across the Central databases of a duplexed Central Controller.
About the IPCC Central Database

The IPCC Central database is the main configuration and call data database for IPCC. It resides on the Central Controller machine. If the Central Controller is duplexed, each physical Central Controller has its own copy of the database. The name of the central database is ipcc_side<A or B>.

Call data is maintained in the Central DB for a period of up to two weeks. Thus, it serves as the "real-time" database for IPCC. Data in excess of two weeks old is transferred to the Historical DB.

The Central database stores:

• Full configuration information for IPCC
• All routing scripts—current and, if you choose to save them, past versions
• Event data
• Call detail data
• Five-minute summary data
• Half-hour historical data

The Central database maintains 5-minute summary and half-hour historical data for each:

• Skill group

The Central database also maintains five-minute summary data for Routing Clients and Scripts and half-hour data for Application Gateways. Although you can view these data in reports, you cannot modify them directly or indirectly.

Administration & WebView Reporting Local Database

Each Administration & WebView Reporting machine has a copy of the Central database configuration data and scripts in its local database. This database is used to make changes to configuration and script data; when you change the IPCC configuration through the IPCC Web Administration Tool, or you create scripts with the Internet Script Editor, the data is written first to the Central Database and then replicated out to the Administration & WebView Reporting local database. As necessary, the Central Controller forwards any changes in historical data to the Historical Data Server (HDS) machine.

The Administration & WebView Reporting Local database is named ipcc_awdb.
The Administration & WebView Reporting local database contains the following information:

- Configuration information (copied from the Central database)
- Scripts (copied from the Central database)
- Real-time data

The real-time client process on the Administration & WebView Reporting machine keeps the real-time data in the local database up-to-date. It receives real-time data from the real-time server approximately every ten seconds. Old real-time data is constantly overwritten by new real-time data.

**Temporary Database**

Because real-time data are written and read frequently, the real-time tables are stored in memory as temporary tables. Although these tables physically reside in the temporary database--TEMPDB--you can access them as if they were in Administration & WebView Reporting local database.

**About the Historical Database**

Administration & WebView Reporting components need to access historical data (half hour data, call detail, etc.). IPCC stores historical data in the Central database on the Central Controller. The Central Controller also forwards historical records to the Historical Data Server (HDS) machine for storage in a special local database--the Historical database. The Historical database resides on the Administration & WebView Reporting machine. It is sized at installation to 14 gigabytes, more than sufficient for ongoing historical data storage requirements. It's database name is ipcc_hds.

In deployments that include two Administration & WebView Reporting machines both serve as the HDS machines.

**Note:** All-in-One deployments do not include or support a Historical database. In these deployments, historical reporting data is served from the Central database.

**About the WebView Database**

The WebView database resides on the Administration & WebView Reporting machine. It stores WebView configuration data (such as saved report definitions)--but not actual report data. The WebView database is sized at installation to 100 megabytes which is more than sufficient to store all WebView configuration data. It's database name is wvdb.
About the Outbound Option Database

The Outbound Option database resides on the machine that includes the Central Controller. The Outbound Option database is sized at installation to 1.4 gigabytes which is more than sufficient to store all Outbound Option data. It's database name is ipce_baA.

Configuration Management Service (CMS)

The Configuration Management Service (CMS) authenticates the connection between IPCC and its database for database writes. It also coordinates the configuration of objects common to both IPCC and to application instances such as Cisco E-Mail Manager and Cisco Collaboration Server. It also authenticates agents when they log in. Common objects are stored both in the application instance local database and the IPCC Central database. The copy of the data in the Central database is used for integrated reporting and for authentication of agents. The copies of the data in the application instance databases is used for application specific reporting and for application operation.

CMS includes the following components:

• A set of client libraries that reside on the application instance system and are called by the application.
• A service process that runs on Administration & WebView Reporting.

The server process reads configuration data from the Administration & WebView Reporting database and writes configuration data to IPCC via the Central Controller API (CCAPI). The CMS client library communicates with the CMS server process using a message bus.


Historical Data Administration

IPCC maintains a database on each side of the Central Controller and a local database on each Administration & WebView Reporting machine. Each database consists of a group of interrelated tables. As you add or update data in the database, you must ensure that logical relationships are maintained. For example, if you delete a call type, you must not leave dialed numbers in the database that reference that call type. If you do, the integrity of the database is broken. The IPCC Web Administration Tool prevents you from making certain changes that disrupt the integrity of the data in the database. However, it cannot prevent all such changes. Usually, if data integrity in the local database is temporarily disrupted, no major problems occur. However, integrity problems in the Central database could cause errors in system processing.
Note: To protect the integrity of the IPCC databases, do not use third-party tools to modify them. These tools do not protect against disruptions of database integrity. (You can use third-party tools to view IPCC data.)

When IPCC is installed, it automatically performs integrity checks to make sure that the database is configured correctly. After that, the integrity of the Central database is maintained by the IPCC software. You do not need to manually check the integrity of the IPCC Central database. If you ever have a problem with data integrity in the Central database, the problem is most likely a software problem that needs to be addressed by your IPCC support provider.

Note: Any manual integrity checks of the central database must involve your IPCC support provider. Do not run the DBCC CHECKDB procedure on the Central database while the IPCC system is running. This procedure will stop the logger process running on the Central Controller.

About the Database Purge Procedure

IPCC initiates a purge process on the Central Controller and the HDS Administration & WebView Reporting machine once every day. The purge process deletes records that are older than a specified number of days. By default, the purge process runs each night at 12:30 A.M. You can specify a different purge schedule on the Database page in the IPCC Web Administration Tool.

<table>
<thead>
<tr>
<th>Historical Tables</th>
<th>Default Retention Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application_Event, Config_Message_Log, Event</td>
<td>14 days</td>
</tr>
<tr>
<td>Logger_Admin, Recovery</td>
<td>30 days</td>
</tr>
<tr>
<td>All other historical tables</td>
<td>14 days in Central Controller, 1095 days in Administration &amp; WebView Reporting</td>
</tr>
</tbody>
</table>
Chapter 14

Increasing Fault Tolerance in an IPCC Enterprise System

This appendix provides information on how to configure IPCC Enterprise for enhanced fault tolerance. For more information on designing and implementing fault tolerance in IPCC Enterprise system, see the Cisco IP Contact Center Enterprise Edition Solution Reference Network Design Guide.

How to Set Up a Recovery Number for Your IPCC System

Cisco recommends setting up your system with a recovery number for fail-over situations. For example, you might forward calls to voice mail. You might also decide to forward calls to another CTI Route Point or dialed number that sends the call to a special recovery script on the system.

Once you have determined an appropriate recovery number for your system, configure Call Forward No Answer and Call Forward Busy on the CTI Route Points for the Agent/IVR Controller and the IP IVR to point to this recovery number.

Also configure the CallForward on Busy (CFB) option on your phones to point to this number as well. You can use the CallManager Bulk Administration Tool to do this for a group of phones, or you can configure each line individually using the CallManager administration Web pages.

How to Improve Failure Detection

The Agent/IVR Controller will detect a failure after two successive heartbeats are missed. You can improve failure detection by reducing the time between heartbeats sent by the CallManager.

You use the Server Heartbeat Interval (sec) field on the CallManager to set the time interval between heartbeats. The default is 30 seconds; Cisco recommends changing this to the minimum value of 5.
To change the heartbeat interval:

**Step 1**  From the Start menu, select Programs -> Cisco JTAPI -> JTAPI Preferences.

**Step 2**  Set the Advanced -> Server Heartbeat Interval (sec) field to 5 seconds.
Chapter 15

Uninstalling and Reinstalling IPCC

How to Uninstall the Controllers and Administration & WebView Reporting

As necessary, you can uninstall the controllers and Administration & WebView Reporting from any machine. Care must be taken not to uninstall a component that is still referenced by other components in an active system.

Note: Uninstalling IPCC will not uninstall the following: the IPCC database, Cisco JTAPI, Servlet Exec, the Sybase EAServer, and the JDK. As desired, the database can be deleted manually in SQLServer. Cisco JTAPI must be uninstalled through Windows Add/Remove Programs. On the Administration & WebView Reporting machine, Servlet Exec, the Sybase EAServer, and the JDK MUST be uninstalled following the 3rd party software uninstallation instructions for System IPCC deployments located in the WebView Installation and Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions.

Step 1
In IPCC Web Administration, on the Machines page, delete the machine you want to uninstall. Always delete a machine prior to uninstalling its IPCC software, even if you later plan to reinstall IPCC on that machine. Failing to do this will cause an condition whereby IPCC Web Administration believes the machine still exists and is properly configured, resulting in communication errors.

Step 2
From the Windows > Control Panel > Add/Remove Programs, select IPCC Enterprise...OR... Insert the System IPCC Enterprise DVD in your machine's DVD drive and run setup.exe from the top level of the DVD.

Note: It is not necessary to stop IPCC services prior to an uninstall, the uninstall program will do this for you.

Step 3
After the uninstall is complete, reboot the machine. In some instances, uninstall may fail to remove the IPCC directory and some of its files. After reboot, you can remove it by deleting this directory: <root>\icm.
How to Re-Install the Controllers and Administration & WebView Reporting

Controller and Administration & WebView Reporting software can be re-installed only if it has first been uninstalled. You cannot re-install the software over itself--rerunning setup over a current install will uninstall the product. Further, Cisco JTAPI, Servlet Exec, the Sybase EAServer, and the JDK MUST be uninstalled prior to a reinstall of IPCC software. Uninstall Cisco JTAPI through Windows Add/Remove Programs. IMPORTANT: On the Administration & WebView Reporting machine, you must uninstall Servlet Exec, the Sybase EAServer, and the JDK following the 3rd party software uninstallation instructions for System IPCC deployments located in the WebView Installation and Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions.

Note: Always delete a machine (in IPCC Web Administration, on the Machines page) prior to uninstalling its IPCC software. Do this even if you later plan to reinstall IPCC on that machine. Failing to do this will cause an condition whereby IPCC Web Administration believes the machine still exists and is properly configured, resulting in communication errors.

During a re-install, if you did not manually delete the old IPCC database, IPCC will be use the old database rather than overwriting it.
System IPCC Enterprise shares many components and functionality in common with Cisco Intelligent Contact Management (ICM). In System IPCC, some of these components have been rebranded, although their functionality remains the same.

While *this* document was produced specifically for System IPCC and reflects this rebranding, it may refer readers to other documents that use the ICM naming conventions for these components. Further, certain utilities available to System IPCC users may also use ICM naming conventions in their interfaces. Therefore, this section maps System IPCC machine types to their ICM equivalents, and also describes ICM objects that are either non-applicable or have been rebranded in System IPCC.

This section contains the following topics:

- System IPCC to ICM Component Mapping, page 133
- System IPCC to ICM Object Mapping, page 134
- System IPCC to ICM Installation Differences, page 134

### System IPCC to ICM Component Mapping

The table below maps System IPCC machine types to their equivalent ICM components.

<table>
<thead>
<tr>
<th>System IPCC Machine Type</th>
<th>Corresponding ICM Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Controller</td>
<td>CallRouter, Logger</td>
</tr>
<tr>
<td>Agent/IVR Controller</td>
<td>System PG, CTI Server, CTI OS Server</td>
</tr>
<tr>
<td>Administration &amp; WebView Reporting</td>
<td>Distributor Admin Workstation, Historical Data Server (HDS), WebView</td>
</tr>
</tbody>
</table>
System IPCC to ICM Object Mapping

Following is a list of ICM objects either not used or renamed in System IPCC:

- While the following ICM objects are supported by system IPCC, they are configured automatically and therefore are not exposed through the configuration tools: labels, persons, device targets, and trunk groups.

- Configuration of translation routes is automatic—no manual configuration is required.

- System IPCC does not support post routing within System IPCC deployment. Post routing is supported between a child System IPCC and its parent in an IPCC Gateway deployment. (See your IPCC Gateway documentation for more information.)

- System IPCC does not support services, sub-skill groups, or Dialed Number Plan configuration.

- System IPCC's call variables are equivalent to ICM's expanded call context variables.

- System IPCC's network IVR is equivalent to ICM's network VRU.

System IPCC to ICM Installation Differences

Following is a list of differences between the way certain shared ICM/System components are installed in System IPCC versus in ICM:

- System IPCC supports a single customer instance per Active Directory Facility OU. This instance is automatically named "ipcc."

- All ICM databases and the Outbound Option database are installed, sized, and configured automatically in System IPCC installs. No manual configuration of these databases is required.

- The IPCC System PG is installed and configured transparently in System IPCC. This is the only Agent PG type supported by System IPCC. No manual configuration of PG client type, PIMs, etc. is required.

- WebView and the WebView 3rd Party Utilities are installed automatically in System IPCC. No manual install of these product components is required. Agent Reporting is automatically enabled in System IPCC; it does not need to be manually enabled. All prospective WebView users must first have an account on the System IPCC’s Active Directory domain. Outbound Option reporting templates are installed automatically and appear in WebView whether Outbound is deployed or not.
Index

3rd party software
requirements....22
abandoned short calls....109
active directory
 supported models....21
Active Directory
troubleshooting....114
Admin Workstation....133
answered short calls....109
bucket intervals
 assigning to call types....108
 creating....108
call flows....16
callrouter....133
call types
 reporting configuration....106
components
 for IPCC, described....13
 multichannel....15
ConAPI....119
Controllers and Administration and WebView Reporting
 uninstalling and reinstalling....131
CTI OS Server....133
CTI Server....133
customer instance....134
database
 connection troubleshooting....119
databases
 automatic installation....134
described....121
 maintaining....121
deployment wizard....62, 68
device targets....134
Distributor AW....133
ECC variables....134
expanded call context variables....134
failure detection....129
fault tolerance
 increasing....129
global options
 for call types....106, 109
hardware requirements....19
HDS....133
Historical Data Server....133
ICM components in IPCC....133
IIS....115
instance....134
internationalization....22
IPCC
 components....13
ipcc instance....134
IPCC Web Administration
troubleshooting....116, 117, 118
JDBC....119
labels....134
licensing....23
localization....22
logger....133
Machine Initiator....114
machines
 configuration requirements by type....63
media routing domain
 reporting configuration....106
MR PG....133
multichannel....15
network vru....134
operating system
requirements....21
Outbound Dialer....133
Outbound Options....15
peripheral ID....120
persons....134
post routing....134
recovery numbers....129
reinstalling....131
reporting
configuring....105
supervisory features....110
server
requirements....19
service levels
reporting configuration....106
service level threshold
assigning to call types....106
assigning to media routing domains....106
assigning to skill groups....106
services....134
short calls....109
skill groups
reporting configuration....106
sub....134
SQLServer....113
sub skill groups....134
System IPCC
components....13
system pg....133, 134
system pg peripheral id....120
Tomcat....115
translation routes....134
troubleshooting....113, 116, 117, 118
trunk groups....134
uninstalling....131
unsupported features....23
version interoperability....22
WebView automatic installation....134
installation location....133
windows requirements....21