IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition
Cisco IPCC Enterprise Edition Release 7.0(0)
May 2007
# Contents

**About This Guide**  
i  
- Purpose  
i  
- Audience  
i  
- Organization  
ii  
- Conventions  
iii  
- Other Publications  
iii  
- Obtaining Documentation  
iii
  - Cisco.com  
  - Product Documentation DVD  
  - Ordering Documentation  

- Documentation Feedback  
iv  
- Cisco Product Security Overview  
v  
  - Reporting Security Problems in Cisco Products  
v  
- Product Alerts and Field Notices  
v  
- Obtaining Technical Assistance  
vi  
  - Cisco Support Website  
  - Submitting a Service Request  
  - Definitions of Service Request Severity  
vii  
- Obtaining Additional Publications and Information  
vii

## Chapter 1

Introduction to Cisco IPCC Enterprise  
1-1  
  - About IPCC Enterprise Edition  
  - About IPCC Enterprise Components  
    - IPCC Enterprise Core Components  
    - IPCC Enterprise Optional Components  
  - Basic IPCC Call Flow  
1-5

## Chapter 2

IPCC Enterprise Platform Specifications  
2-1  
  - IPCC Enterprise Server Platforms  
  - About IPCC Enterprise Operating System Requirements  
  - About IPCC Enterprise Network and Active Directory Domain Requirements  
  - About IPCC Enterprise 3rd Party Software Requirements  
  - About IPCC Enterprise Component Version Interoperability  
2-3
<table>
<thead>
<tr>
<th>Chapter 3</th>
<th>Overview of Installation and Configuration Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Licensing Requirements and System Limitations 2-4</td>
</tr>
<tr>
<td></td>
<td>About IPCC Internationalization and Localization Support 2-4</td>
</tr>
<tr>
<td></td>
<td>About Non-Supported Component Features in an IPCC Environment 2-4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 3</th>
<th>Overview of Installation and Configuration Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hardware Installation Checklist 3-1</td>
</tr>
<tr>
<td></td>
<td>IPCC Enterprise Component Software Installation Checklist 3-2</td>
</tr>
<tr>
<td></td>
<td>IPCC Enterprise Component Software Configuration Tasks 3-6</td>
</tr>
<tr>
<td></td>
<td>IPCC Enterprise Production Environment Worksheet 3-6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Installing and Configuring Cisco CallManager for IPCC Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About Cisco CallManager 4-2</td>
</tr>
<tr>
<td></td>
<td>How to Install Cisco CallManager for IPCC Enterprise 4-2</td>
</tr>
<tr>
<td></td>
<td>How to Configure CallManager for IPCC Enterprise 4-3</td>
</tr>
<tr>
<td></td>
<td>About the CallManager Administration Utility 4-4</td>
</tr>
<tr>
<td></td>
<td>How to Configure Agent IP Phones for IPCC Enterprise 4-4</td>
</tr>
<tr>
<td></td>
<td>How to Configure Agent IP Phones on the CallManager 4-4</td>
</tr>
<tr>
<td></td>
<td>How to Set the Agent IP Phone Configuration on the IP Phone 4-5</td>
</tr>
<tr>
<td></td>
<td>About the CallManager Extension Mobility Feature 4-5</td>
</tr>
<tr>
<td></td>
<td>How to Configure CTI Route Points 4-6</td>
</tr>
<tr>
<td></td>
<td>How to Configure CTI Ports 4-7</td>
</tr>
<tr>
<td></td>
<td>How to Configure JTAPI Users for the JTAPI Phones, CallManager PG and IP IVR 4-7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Installing and Configuring Cisco IP IVR for IPCC Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About IP IVR 5-2</td>
</tr>
<tr>
<td></td>
<td>How to Install IP IVR for IPCC Enterprise 5-2</td>
</tr>
<tr>
<td></td>
<td>About IP IVR Installation Prerequisites 5-3</td>
</tr>
<tr>
<td></td>
<td>How to Configure IP IVR for IPCC Enterprise 5-3</td>
</tr>
<tr>
<td></td>
<td>About the CRA Administration Utility 5-4</td>
</tr>
<tr>
<td></td>
<td>How to Configure the Directory Profile 5-4</td>
</tr>
<tr>
<td></td>
<td>How to Configure the JTAPI User on the IP IVR System 5-6</td>
</tr>
<tr>
<td></td>
<td>How to Configure CTI Port Groups 5-6</td>
</tr>
<tr>
<td></td>
<td>How to Configure the ICM Subsystem 5-7</td>
</tr>
<tr>
<td></td>
<td>How to Configure and Upload VRU Scripts 5-9</td>
</tr>
<tr>
<td></td>
<td>About Translation Routing and Post Routing 5-9</td>
</tr>
<tr>
<td></td>
<td>About Translation Routing 5-9</td>
</tr>
<tr>
<td></td>
<td>About Post Routing 5-10</td>
</tr>
<tr>
<td></td>
<td>How to Configure IP IVR for ICM Translation Routing 5-10</td>
</tr>
<tr>
<td>Chapter 6: Installing and Configuring Cisco ICM for IPCC Enterprise</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>How to Configure IP IVR for ICM Post Routing</td>
<td>5-11</td>
</tr>
<tr>
<td>How to Configure and Start the Application Engine</td>
<td>5-12</td>
</tr>
<tr>
<td>How to Verify and Update the JTAPI Client</td>
<td>5-12</td>
</tr>
<tr>
<td>About Cisco Intelligent Contact Management Software</td>
<td>6-2</td>
</tr>
<tr>
<td>Installing and Configuring Cisco ICM for IPCC Enterprise</td>
<td>6-1</td>
</tr>
<tr>
<td>How to Install ICM for IPCC Enterprise</td>
<td>6-2</td>
</tr>
<tr>
<td>How to Enable ICM Outbound Option During ICM Installation</td>
<td>6-3</td>
</tr>
<tr>
<td>About ICM Installation Prerequisites</td>
<td>6-3</td>
</tr>
<tr>
<td>How to Configure ICM for IPCC Enterprise</td>
<td>6-3</td>
</tr>
<tr>
<td>About ICM Configuration Tasks</td>
<td>6-3</td>
</tr>
<tr>
<td>About ICM Components</td>
<td>6-2</td>
</tr>
<tr>
<td>About the ICM Configuration Manager</td>
<td>6-5</td>
</tr>
<tr>
<td>About the ICM Bulk Configuration Tool</td>
<td>6-5</td>
</tr>
<tr>
<td>How to Configure Agent Desk Settings</td>
<td>6-6</td>
</tr>
<tr>
<td>About Re-route on No Answer</td>
<td>6-6</td>
</tr>
<tr>
<td>How to Configure Agent Desk Settings</td>
<td>6-8</td>
</tr>
<tr>
<td>How to Create a Network VRU</td>
<td>6-9</td>
</tr>
<tr>
<td>About IPCC Peripheral Gateways</td>
<td>6-9</td>
</tr>
<tr>
<td>How to Configure and Install the System PG</td>
<td>6-10</td>
</tr>
<tr>
<td>How to Configure the System PG</td>
<td>6-10</td>
</tr>
<tr>
<td>How to Configure the System PG Peripheral</td>
<td>6-11</td>
</tr>
<tr>
<td>How to Install the System PG</td>
<td>6-13</td>
</tr>
<tr>
<td>How to Configure and Install the Generic PG</td>
<td>6-15</td>
</tr>
<tr>
<td>How to Configure the Generic PG</td>
<td>6-16</td>
</tr>
<tr>
<td>How to Configure the CallManager Peripheral</td>
<td>6-16</td>
</tr>
<tr>
<td>How to Configure the VRU Peripheral</td>
<td>6-18</td>
</tr>
<tr>
<td>How to Install the Generic PG</td>
<td>6-19</td>
</tr>
<tr>
<td>How to Install the Cisco JTAPI Client on the System or Generic PG</td>
<td>6-21</td>
</tr>
<tr>
<td>How to Configure and Install the Media Routing PG</td>
<td>6-22</td>
</tr>
<tr>
<td>How to Configure the MR-PG and Peripherals</td>
<td>6-22</td>
</tr>
<tr>
<td>How to Configure the MR PG Peripherals</td>
<td>6-22</td>
</tr>
<tr>
<td>How to Install the MR-PG</td>
<td>6-23</td>
</tr>
<tr>
<td>How to Configure Trunk Groups</td>
<td>6-24</td>
</tr>
<tr>
<td>How to Configure the Network VRU Bank</td>
<td>6-26</td>
</tr>
<tr>
<td>How to Configure Services</td>
<td>6-26</td>
</tr>
<tr>
<td>How to Configure Skill Groups</td>
<td>6-27</td>
</tr>
<tr>
<td>About Default Skill Groups</td>
<td>6-28</td>
</tr>
<tr>
<td>About the “ICM picks the agent” Skill Group Attribute</td>
<td>6-28</td>
</tr>
</tbody>
</table>
CHAPTER 9
Installing Agent and Supervisor Desktops for IPCC Enterprise
About Agent and Supervisor Desktops for IPCC Enterprise
About Agent and Supervisor Desktop Installation Prerequisites
About CTI OS Silent Monitor Feature Prerequisites
About Agent and Supervisor Desktop Installation Tasks
How to Install the CTI OS Server
How to Create a User for ODBC File Data Source Name
How to Create and Configure an ODBC file Data Source Name
How to Install CTI OS Server
How to Install and Configure CTI OS Desktops
How to Install the CTI OS Supervisor Desktop
How to Install the CTI OS Agent Desktop
How to Install and Configure the CAD Agent and Supervisor Desktops
Cisco Agent Desktop (CAD) Pre-Installation Requirements
How to Install and Configure the Cisco Agent Desktop Applications
How to Start CTI OS Services After Installation

CHAPTER 10
Installing and Configuring Cisco Multichannel Components for IPCC Enterprise
About IPCC Enterprise Multichannel Components
About Cisco Collaboration Server
About Cisco E-Mail Manager
How to Install Multichannel Components for IPCC Enterprise
About Multichannel Installation Prerequisites
How to Configure Multichannel Components for IPCC Enterprise
About Multichannel Configuration Tasks
About ICM Configuration for Multichannel Components
About Media Routing Peripheral Gateways
About Media Routing Domains and Media Classes
About Multichannel Agents
About Application Instances
About Multichannel Skill Groups
About Universal Queue and Multichannel Routing Scripts
How to Configure Media Routing Domains
How to Configure Application Instances
How to Establish Administration Connections
How to Set ECC (Expanded Call Context) Variables
How to Write ICM Routing Scripts for Multichannel Options
How to Configure Cisco Web Collaboration Server for ICM Integration
How to Configure Cisco Media Blender for ICM Integration  10-12
How to Configure Cisco E-Mail Manager for ICM Integration  10-12

CHAPTER 11
Configuring Reporting for IPCC Enterprise  11-1
How to Configure Reporting for IPCC Enterprise  11-1
About Reporting Configuration Prerequisites  11-2
About IPCC Reporting Configuration Tasks  11-2
How to Configure Agent Reporting  11-2
   How to Enable Agent Reporting for the CallManager PG  11-2
   How to Specify the Admin Workstation Distributor for CallManager PIMs  11-3
How to Configure Service Levels  11-3
   How to Set the System Service Level for Call Types  11-3
   How to Set Service Levels for Call Types  11-4
   How to Set the Service Levels for Services  11-4
How to Configure Bucket Intervals  11-4
   How to Define Bucket Intervals  11-4
   How to Set the System Bucket Interval  11-5
   How to Set Bucket Intervals for Call Types  11-5
How to Configure IVR Applications  11-5
How to Configure Short Calls  11-6
   How to Configure Short Calls for Call Types  11-6
   How to Configure Short Calls for Services  11-6
About Other Reporting Setup Options  11-7
   About IPCC Supervisory Features  11-7
   About Agent Transfer and Conferencing  11-7

APPENDIX A
IPCC Enterprise Checklists and Worksheets  A-1
IPCC Enterprise Hardware Installation Tasks  A-2
IPCC Enterprise Component Software Installation Tasks  A-3
IPCC Enterprise Component Software Configuration Tasks  A-6
   CallManager Configuration Tasks  A-7
   IP IVR Configuration Tasks  A-8
   ICM Configuration Tasks  A-8
   Outbound Option Configuration Tasks  A-9
   CVP Configuration Tasks  A-9
   Agent and Supervisor Desktop Configuration Tasks  A-10
   Multichannel Configuration Tasks  A-10
   IPCC Reporting Configuration Tasks  A-11
IPCC Enterprise Configuration Values Worksheets  A-11
About This Guide

Purpose

Welcome to the *IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition*. This guide provides information to help you understand and configure the IPCC Enterprise system in both production and laboratory environments.

The Cisco IPCC Enterprise solution consists of multiple software and hardware components that must be installed, configured, and integrated with each other. This guide describes each of those components and for each provides the installation and configuration information required for their deployment in an IPCC environment. *This guide provides IPCC-specific information only.* It does not provide generic non-IPCC installation and configuration information for individual components. As appropriate, this guide directs the reader to additional publications for this information.

The configuration information in this guide pertains to initial IPCC setup only. For post-deployment configuration options and instructions, see the *IPCC Administration Guide for Cisco IPCC Enterprise Edition*.

This guide provides information to help you understand and configure the IPCC Enterprise system in both production and laboratory environments.

Audience

This guide is written for anyone who is responsible for setting up and configuring an IPCC Enterprise production or laboratory system and the products of which it is comprised.
## Organization

This guide contains the following chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Introduction to Cisco IPCC Enterprise”</td>
<td>This chapter provides a brief description of the IPCC Enterprise system and an explanation of its components.</td>
</tr>
<tr>
<td>Chapter 2, “IPCC Enterprise Platform Specifications”</td>
<td>This chapter provides hardware and software specifications for IPCC Enterprise components. It also provides a list of component features not supported when components are deployed as part of an IPCC Enterprise system.</td>
</tr>
<tr>
<td>Chapter 3, “Overview of Installation and Configuration Tasks”</td>
<td>This chapter includes task checklists designed to help you track your progress as you install and configure IPCC.</td>
</tr>
<tr>
<td>Chapter 4, “Installing and Configuring Cisco CallManager for IPCC Enterprise”</td>
<td>This chapter describes how to install and configure Cisco CallManager software in laboratory and production environments.</td>
</tr>
<tr>
<td>Chapter 5, “Installing and Configuring Cisco IP IVR for IPCC Enterprise”</td>
<td>This chapter describes how to install and configure IP IVR software in laboratory and production environments. Read and follow the instructions in this chapter if you are using IP IVR (as opposed to CVP) for queuing.</td>
</tr>
<tr>
<td>Chapter 6, “Installing and Configuring Cisco ICM for IPCC Enterprise”</td>
<td>This chapter describes how to install and configure ICM software components.</td>
</tr>
<tr>
<td>Chapter 7, “Installing and Configuring Outbound Option for IPCC Enterprise”</td>
<td>This chapter describes how to configure the optional Outbound Option feature for IPCC Enterprise.</td>
</tr>
<tr>
<td>Chapter 8, “Installing and Configuring Cisco CVP for IPCC Enterprise”</td>
<td>This chapter describes how to install and configure CVP software in laboratory and production environments. Read and follow the instructions in this chapter if you are using CVP (as opposed to IP IVR) for queuing.</td>
</tr>
<tr>
<td>Chapter 9, “Installing Agent and Supervisor Desktops for IPCC Enterprise”</td>
<td>This chapter describes how to install and configure Cisco Agent Desktop and CTI OS Agent Desktop and IPCC Supervisor Desktop.</td>
</tr>
<tr>
<td>Chapter 10, “Installing and Configuring Cisco Multichannel Components for IPCC Enterprise”</td>
<td>This chapter describes how to install and configure Cisco Multichannel software for the IPCC Enterprise systems.</td>
</tr>
<tr>
<td>Chapter 11, “Configuring Reporting for IPCC Enterprise”</td>
<td>This chapter describes tasks required to configure reporting for your IPCC Enterprise system.</td>
</tr>
<tr>
<td>Appendix A, “IPCC Enterprise Checklists and Worksheets”</td>
<td>This appendix provides a compilation of the IPCC installation and configuration checklists and worksheets appearing in this guide. These can be used to guide you through an IPCC Enterprise deployment.</td>
</tr>
</tbody>
</table>
Conventions

This manual uses the following conventions:

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boldface type is used for user entries, keys, buttons, and folder and submenu names.</td>
<td>Click <strong>Logger</strong>, then click the <strong>Edit</strong> button in the Instance Components section.</td>
</tr>
<tr>
<td>Italic type indicates one of the following:</td>
<td>• A <em>skill group</em> is a collection of agents who share similar skills.</td>
</tr>
<tr>
<td>• A newly introduced term</td>
<td>• <em>Do not</em> use the numerical naming convention that is used in the predefined templates (for example, <strong>persvc01</strong>).</td>
</tr>
<tr>
<td>• For emphasis</td>
<td>• IF (<em>condition</em>, <em>true-value</em>, <em>false-value</em>)</td>
</tr>
<tr>
<td>• A generic syntax item that you must replace with a specific value</td>
<td>• For more information, see the <em>Cisco ICM Enterprise Edition Database Schema Handbook</em>.</td>
</tr>
<tr>
<td>• A title of a publication</td>
<td></td>
</tr>
<tr>
<td>An arrow (&gt;) indicates an item from a pull-down menu.</td>
<td>The Save command from the File menu is referenced as <strong>File &gt; Save</strong>.</td>
</tr>
</tbody>
</table>

Other Publications

For additional information about Cisco Intelligent Contact Management (ICM) software, see the Cisco web site listing ICM documentation.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

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 library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:
http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:
http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:
http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

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 do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco
A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

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

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


**Reporting Security Problems in Cisco Products**

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

- For emergencies only — security-alert@cisco.com

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

- For nonemergencies — psirt@cisco.com

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

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

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (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 encryption key 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 to find other means of encrypting the data before sending any sensitive material.

**Product Alerts and Field Notices**

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements 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.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:
Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support 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 Support Website

The Cisco Support 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:


Access to all tools on the Cisco Support 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

Before you submit a request for service online or by phone, use the Cisco Product Identification Tool to locate your product serial number. You can access this tool from the Cisco Support website by clicking the Get Tools & Resources link, clicking the All Tools (A-Z) tab, and then choosing Cisco Product Identification Tool from the alphabetical list. This 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.

Tip

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the Advanced Search link next to the Search box on the resulting page and then click the Technical Support & Documentation radio button.

To provide feedback about the Cisco.com website or a particular technical document, click Contacts & Feedback at the top of any Cisco.com web page.
Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

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

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

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

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

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

http://www.ciscopress.com

*Internet Protocol Journal* is a quarterly journal published by Cisco 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, as well as customer support services, can be obtained at this URL:


Networking Professionals Connection is an interactive website where networking professionals 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

“What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

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

CHAPTER 1

Introduction to Cisco IPCC Enterprise

This chapter provides a brief description of IPCC Enterprise and an explanation of its components. It contains these sections:

- About IPCC Enterprise Edition, page 1-1
- About IPCC Enterprise Components, page 1-1
- Basic IPCC Call Flow, page 1-5

About IPCC Enterprise Edition

Cisco IPCC Enterprise is part of the Cisco Architecture for Voice, Video, and Integrated Data (AVVID). IPCC 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. IPCC Enterprise sites also can be used as service bureaus. This guide explains how to set up IPCC Enterprise in a laboratory environment and in production environments including single-site, multi-site, and service bureau.

About IPCC Enterprise Components

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

The core components are required parts of all IPCC Enterprise deployments:

<table>
<thead>
<tr>
<th>IPCC Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco CallManager</td>
<td>Cisco CallManager provides features comparable with those of a traditional PBX system and handles the switching requirements of IPCC. It allows deployment of voice applications and the integration of telephony systems with Intranet applications. Cisco CallManager software must be installed on a Cisco Media Convergence Server (MCS).</td>
</tr>
</tbody>
</table>
| Cisco IP IVR or Cisco CVP | Cisco IP IVR and Cisco CVP both provide Interactive Voice Response (IVR) and queuing capability in IPCC. You select which of these IVR systems to deploy in your IPCC.  
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. |
| Cisco ICM software   | Cisco ICM software provides intelligent multichannel contact routing and ACD functionality, including monitoring and controlling agent state, CTI capabilities, and gathering real-time and historical data for reporting in IPCC Enterprise.  
The ICM software includes the CallRouter, Logger, Peripheral Gateway(s) for CallManager and VRU PIMs, CTI Server, and Admin Workstation. ICM software also provides Outbound Option, which enables agents to make outbound calls to customers, and Media Routing Peripheral Gateways (MR-PG) to connect to multichannel applications. |
| Cisco CTI Object Server CTI IOS or CAD desktops | 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 application to deploy in IPCC.  
CTI OS includes the CTI OS Server, 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. |

In addition to these components, IPCC includes Voice-over-IP (VoIP) gateways, and Peripheral Gateway with CallManager and IP-IVR or CVP PIMs.
The following figure shows the core components of the IPCC Enterprise:

![IPCC Enterprise Components Diagram]

## IPCC Enterprise Optional Components

The following optional software components can be (but are not required to be) deployed in IPCC Enterprise. This group of components provide Web and E-mail interactivity to IPCC. They are referred to collectively as the *Multichannel* components.

<table>
<thead>
<tr>
<th>IPCC Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Collaboration Server</td>
<td>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 ICM CallRouter via the MR-PG, and the CallRouter selects the agent to handle the request.</td>
</tr>
<tr>
<td>Cisco Media Blender</td>
<td>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 ICM MR-PG inside the firewall.</td>
</tr>
<tr>
<td>Cisco Dynamic Content Adapter</td>
<td>Cisco Dynamic Content Adapter (DCA) is an intelligent Web proxy caching server that allows the Collaboration Server users to share secure, personalized, live, interactive, and transactional Web content.</td>
</tr>
<tr>
<td>Cisco E-Mail Manager</td>
<td>Cisco E-Mail Manager (CEM) manages high volume 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 ICM CallRouter via the MR-PG, and the CallRouter routes the request to an available agent.</td>
</tr>
</tbody>
</table>
The following figure shows the optional multichannel components in an IPCC Enterprise deployment:
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 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.

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 IPCC controller.
4. IPCC runs routing script. No available agent found, so IP IVR label returned from routing script.
5. IPCC controller instructs Cisco CallManager to transfer call to IP IVR, and Cisco CallManager does as instructed.
6. IP IVR notifies IPCC controller that call has arrived.
7. IPCC controller instructs IP IVR to play queue announcements.
8. Agent becomes ready (completed previous call or just went ready).
9. IPCC controller 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.

Cisco IP Contact Center Solution Reference Network Design Guide
This chapter provides hardware and software specifications for IPCC Enterprise components. It also provides a list of component features not supported when components are deployed as part of IPCC Enterprise.

This chapter contains these sections:

- IPCC Enterprise Server Platforms, page 2-1
- About IPCC Enterprise Operating System Requirements, page 2-2
- About IPCC Enterprise Network and Active Directory Domain Requirements, page 2-3
- About IPCC Enterprise 3rd Party Software Requirements, page 2-3
- About IPCC Enterprise Component Version Interoperability, page 2-3
- Licensing Requirements and System Limitations, page 2-4
- About IPCC Internationalization and Localization Support, page 2-4
- About Non-Supported Component Features in an IPCC Environment, page 2-4

**IPCC Enterprise Server Platforms**

IPCC 7.0(0) components are supported only on Cisco MCS or MCS-equivalent servers. See the *Cisco ICM/IPCC Enterprise 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 table below provides general guidelines on which IPCC components can be installed on the same machine. Refer to the *Cisco IP Contact Center Solution Reference Network Design Guide* for detailed deployment models, performance limitations, network considerations, and installation options.
Always install IPCC components on a "clean" machine—that is, one which has a fresh install of the operating system and any prerequisite software. Under no circumstances should IPCC components be installed on a domain controller or DNS server.

### IPCC Enterprise Component | Hardware Installation Notes
---|---
CallManager | Install on its own machine. Do not install other IPCC Enterprise components on the CallManager.
ICM | Install ICM software components as duplexed (Side A and Side B) to ensure fault tolerance. Install the ICM Logger on a separate machine than other ICM software components. Typically, though not required, the CTI Server is installed on the same machine as the IPCC PG.
IP IVR | Do not install IP IVR on an ICM Logger or Admin Workstation.
CTI OS and CAD | Install the CTI OS Agent and Supervisor Desktops on different machines.
Cisco Collaboration Server | Install Collaboration Server database server and client on separate machines. Do not install the Cisco Collaboration Server on the same machine as the Dynamic Content Adapter.
Cisco E-Mail Manager | Install E-Mail Manager database server and client on separate machines.
Dynamic Content Adapter | Install the Dynamic Content Adapter on a separate machine. Do not install the Dynamic Content Adapter on the same machine as Cisco Collaboration Server.
Cisco Media Blender | 

## About IPCC Enterprise Operating System Requirements

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

- For Call Manager, see the *Call Manager Compatibility Matrix* at [http://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/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm)
About IPCC Enterprise Network and Active Directory Domain Requirements

IPCC 7.0(0) components require a Windows Active Directory domain. See the Staging Guide for Cisco ICM/IPCC Enterprise & 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 Solution Reference Network Design Guide.

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.

Note

See the Cisco ICM/IPCC Enterprise 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>Cisco CallManager</td>
<td>Installing Cisco CallManager</td>
</tr>
<tr>
<td>Cisco IP IVR</td>
<td>Cisco IP IVR Installation Guide</td>
</tr>
<tr>
<td>Cisco ISN</td>
<td>Cisco Internet Service Node Installation Guide</td>
</tr>
<tr>
<td>Cisco ICM software</td>
<td>ICM Installation Guide for Cisco ICM Enterprise Edition</td>
</tr>
<tr>
<td>Cisco CTI Object</td>
<td>CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise &amp; Hosted Editions</td>
</tr>
<tr>
<td>Server</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td></td>
</tr>
<tr>
<td>Cisco Media Blender</td>
<td>Cisco Media Blender Installation Guide for Cisco ICM/IPCC Enterprise &amp; Hosted Editions</td>
</tr>
<tr>
<td>Cisco Dynamic</td>
<td>Cisco Dynamic Content Adapter Installation and</td>
</tr>
<tr>
<td>Content Adapter</td>
<td>Integration Guide</td>
</tr>
<tr>
<td>Cisco E-Mail Manager</td>
<td>Cisco E-Mail Manager Installation and Configuration</td>
</tr>
<tr>
<td></td>
<td>Guide for Cisco ICM/IPCC Enterprise &amp; Hosted Editions</td>
</tr>
</tbody>
</table>

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: http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/prod_technical_documentation.html
Chapter 2      IPCC Enterprise Platform Specifications

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 IPCC Internationalization and Localization Support

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

About Non-Supported Component Features in an IPCC Environment

This section lists features of individual components that are not supported when these components are used in an IPCC Enterprise deployment.

- IPCC Enterprise does not support CRS clustering (duplexed IP IVRs that failover to the same CTI route points).
- CRS 4.0 (IP IVR) does not allow multiple clusters to share the repository profile for scripts.
- IPCC Enterprise 7.0 does not support partitioning.

Prior to installing and configuring IPCC Enterprise components, consult the ICM/IPCC Enterprise 7.0 Release Notes for a list of any additional component features or configurations not supported in an IPCC Enterprise environment. Cisco Call Manager in particular may have features that cannot be used within IPCC Enterprise.

Overview of Installation and Configuration Tasks

Setting up IPCC Enterprise involves a significant number of installation and configuration tasks. This chapter includes task checklists designed to help you track your progress as you install and configure IPCC. These checklists apply to both production and laboratory deployments.

This chapter contains these sections:

- Hardware Installation Checklist, page 3-1
- IPCC Enterprise Component Software Installation Checklist, page 3-2
- IPCC Enterprise Component Software Configuration Tasks, page 3-6
- IPCC Enterprise Production Environment Worksheet, page 3-6

Hardware Installation Checklist

This section lists the basic order or IPCC component hardware installation. For hardware installation instructions, see the documentation packaged with each component.

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install the Media Convergence Server(s) for Cisco CallManager and IP IVR (if you are using IP IVR rather than CVP in your IPCC).</td>
<td>Hardware and OS requirements for these servers are available from the Hardware Bill of Materials (see link below table).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network architecture requirements are described in the Cisco IP Contact Center Solution Reference Network Design Guide.</td>
<td></td>
</tr>
</tbody>
</table>
### IPCC Enterprise Component Software Installation Checklist

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

#### Notes

See the *IPCC Compatibility Guide* for the list of Cisco IP Phone and IPCC component (e.g., ICM, 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 Compatibility Guide is available from cisco.com at: [http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/prod_technical_documentation.html](http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/prod_technical_documentation.html)

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Install the servers for CallManager, IP IVR (if deploying), ICM, PG, CVP (if deploying), CT IOS, and Multichannel applications.</td>
<td>Hardware and OS requirements for these servers are available from the Hardware Bill of Materials (see link below table).&lt;br&gt;Network architecture requirements are described in the <em>Cisco IP Contact Center Solution Reference Network Design Guide</em>.</td>
</tr>
<tr>
<td>3. 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.&lt;br&gt;Refer to the user documentation for your phone for information on IP address configuration requirements.&lt;br&gt;Refer to the <em>IPCC Compatibility Guide</em> for a list of supported IP Phones.</td>
</tr>
</tbody>
</table>

### IPCC Enterprise Component Software Installation Checklist

<table>
<thead>
<tr>
<th>Task</th>
<th>IPCC Installation Prerequisites</th>
<th>IPCC Installation Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install CallManager</td>
<td>There are no IPCC-specific installation prerequisites for CallManager.</td>
<td>There are no IPCC-specific installation instructions for CallManager.</td>
</tr>
</tbody>
</table>
| 2. Install IP IVR (if IP IVR will be used for queueing). | 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 JTAPI 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 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 ICM 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. See Chapter 5, “Installing and Configuring Cisco IP IVR for IPCC Enterprise” for instructions. |
### IPCC Installation and Configuration Guide

#### IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition

### Chapter 3  Overview of Installation and Configuration Tasks

#### IPCC Enterprise Component Software Installation Checklist

<table>
<thead>
<tr>
<th>Task</th>
<th>IPCC Installation Prerequisites</th>
<th>IPCC Installation Notes</th>
</tr>
</thead>
</table>
| 3.   | Install ICM software, which includes the CallRouter, Logger, Admin Workstation, and Historical Data Server (HDS) database. | Install 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 a CallManager PG JTAPI user and associated the user with CTI Route Point(s) and CTI Port(s).  
- Enabled CTI for the CallManager PG user.  
Install IP IVR if your IPCC Enterprise will use IP IVR for queueing. 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. | There are no IPCC-specific installation instructions for ICM.  
If you will be deploying the Outbound Option, see Chapter 6, “Installing and Configuring Cisco ICM for IPCC Enterprise” for instructions on enabling Outbound Option during ICM installation. |
| 4.   | Install the System or Generic PG. | You must configure the PG before installing it. Generally speaking, you would use the:  
System PG if you are deploying IP IVR.  
Generic PG if you are deploying CVP. | |
| 5.   | Install JTAPI Client on the System or Generic PG. | Before installing the JTAPI Client, you must configure the Generic PG. | |
| 6.   | Install the Media Routing PG (MR-PG) if deploying Multichannel options and/or Outbound Option. | Before installing the MR-PG, you must configure it in ICM. | |
| 7.   | Install the CVP software (if CVP will be used for queueing). | Install Cisco CallManager. On CallManager, you must have configured the CVP Voice Browser as a Gateway on Cisco CallManager.  
Install Cisco ICM software and the PG containing the VRU PIM(s). | If you are deploying an IPCC Enterprise laboratory system, you can install all CVP components on a single machine and must install all components at the same time.  
If you are deploying an IPCC Enterprise production system, you can install individual components on different machines. To maximize performance, do not install the Voice Browser or Application Server on the Media Server, to which you copy System Media Files. |
### Chapter 3  Overview of Installation and Configuration Tasks

#### IPCC Enterprise Component Software Installation Checklist

<table>
<thead>
<tr>
<th>Task</th>
<th>IPCC Installation Prerequisites</th>
<th>IPCC Installation Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>Install CTI Server.</td>
<td>Install and configure CallManager. Install and configure ICM. Install and configure IP IVR or CVP. The CTI Server is an ICM component that allows an external CTI application to communicate with a PG. The CTI Server is part of the Cisco Enterprise CTI product. You can install the CTI Server on the same machine as the Peripheral Gateway software or on a separate machine.</td>
</tr>
<tr>
<td>9.</td>
<td>Install CTI OS software or CAD software, depending on which agent/supervisor desktop software you are deploying.</td>
<td>Install CTI Server.</td>
</tr>
<tr>
<td>10.</td>
<td>Optionally, install the Cisco Collaboration Server software.</td>
<td>Install and configure ICM.</td>
</tr>
<tr>
<td>11.</td>
<td>If you have installed the Cisco Collaboration Server, optionally install Dynamic Content Adapter.</td>
<td>Install and configure Cisco Collaboration Server.</td>
</tr>
<tr>
<td>12.</td>
<td>If you have installed the Cisco Collaboration Server, optionally, install Cisco Media Blender.</td>
<td>Install and configure Cisco Collaboration Server.</td>
</tr>
</tbody>
</table>

*Installing Cisco CallManager Guide
Cisco Customer Response Solutions Getting Started Guide (for IP IVR installation)
Cisco Internet Service Node Installation Guide
ICM Installation Guide for Cisco ICM Enterprise Edition
CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions
Installation Guide: Cisco Desktop Product Suite
Cisco Collaboration Server Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*
Subsequent chapters in this book guide you through configuring each IPCC component/functionality area. Each chapter 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:

<table>
<thead>
<tr>
<th>IPCC Configuration Task</th>
<th>Described In</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure CallManager</td>
<td>Chapter 4, “Installing and Configuring Cisco CallManager for IPCC Enterprise”</td>
</tr>
<tr>
<td>2. Configure IP IVR (if deployed)</td>
<td>Chapter 5, “Installing and Configuring Cisco IP IVR for IPCC Enterprise”</td>
</tr>
<tr>
<td>3. Configure ICM</td>
<td>Chapter 6, “Installing and Configuring Cisco ICM for IPCC Enterprise”</td>
</tr>
<tr>
<td>4. Configure the Outbound Option feature</td>
<td>Chapter 7, “Installing and Configuring Outbound Option for IPCC Enterprise”</td>
</tr>
<tr>
<td>5. Configure CVP (if deployed)</td>
<td>Chapter 8, “Installing and Configuring Cisco CVP for IPCC Enterprise”</td>
</tr>
<tr>
<td>6. Configure Agent And Supervisor Desktops</td>
<td>Chapter 9, “Installing Agent and Supervisor Desktops for IPCC Enterprise”</td>
</tr>
<tr>
<td>7. Configure Multichannel applications (if deployed)</td>
<td>Chapter 10, “Installing and Configuring Cisco Multichannel Components for IPCC Enterprise”</td>
</tr>
<tr>
<td>8. Configure reporting</td>
<td>Chapter 11, “How to Configure Reporting for IPCC Enterprise”</td>
</tr>
</tbody>
</table>

Note: A compilation of the component/feature configuration checklists used throughout these chapters is available in Appendix A, “IPCC Enterprise Checklists and Worksheets.”

**IPCC Enterprise Production Environment Worksheet**

You can use the table below as a worksheet to record the values you enter on each IPCC Enterprise component during installation and configuration. In the table, grey cells indicate configuration items that do not pertain to a specific component.

If the worksheet does not contain enough rows for you to enter all of your configuration values (for example, you configure 30 agents and the worksheet contains only two rows for agents), you can use the worksheet to indicate a file containing all of the values for that item.
Note: A similar worksheet for laboratory installations is provided in Appendix B, “Setting Up an IPCC Enterprise Laboratory System.”

<table>
<thead>
<tr>
<th>Item</th>
<th>CallManager</th>
<th>IP IVR</th>
<th>CVP</th>
<th>ICM</th>
<th>CCS &amp; CEM</th>
<th>CTI OS</th>
<th>CAD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Route Point</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Route Point</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Route Point</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM JTAPI User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP IVR JTAPI User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Port Group number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IVR Flow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IVR Flow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VRU Connection Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM PG Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**IPCC Enterprise Production Environment Worksheet**

<table>
<thead>
<tr>
<th>Item</th>
<th>CallManager</th>
<th>IP IVR</th>
<th>CVP</th>
<th>ICM</th>
<th>CCS &amp; CEM</th>
<th>CTI OS</th>
<th>CAD</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM PIM Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Controller ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peripheral ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP IVR PIM Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Controller ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peripheral ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Server Connection Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network VRU Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP IVR Network Trunk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP IVR Trunk Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP IVR TG Peripheral#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM PG Peripheral Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM PG Network Trunk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM PG Trunk Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MR VRU Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MR PG Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collaboration MR PIM Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Controller ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>CallManager</td>
<td>IP IVR</td>
<td>CVP</td>
<td>ICM</td>
<td>CCS &amp; CEM</td>
<td>CTI OS</td>
<td>CAD</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
<td>--------</td>
<td>-----</td>
<td>-----</td>
<td>-----------</td>
<td>--------</td>
<td>-----</td>
</tr>
<tr>
<td>Peripheral ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-Mail Manager MR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIM Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Controller ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peripheral ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blended Agent PIM Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Controller ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peripheral ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BA Dialer Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BA Dialer Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BA Dialer Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Routing Domains</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ConAPI Connections</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(registry port)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SVC Virtual Ext.#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skill Group #1 Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skill Group Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG Virtual Ext.#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### IPCC Enterprise Production Environment Worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>CallManager</th>
<th>IP IVR</th>
<th>CVP</th>
<th>ICM</th>
<th>CCS &amp; CEM</th>
<th>CTI OS</th>
<th>CAD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill Group #2 Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skill Group Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG Virtual Ext.#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This chapter describes how to install and configure Cisco CallManager for the IPCC Enterprise system. It contains these sections:

- **About Cisco CallManager**, page 4-2
- **How to Install Cisco CallManager for IPCC Enterprise**, page 4-2
- **How to Configure CallManager for IPCC Enterprise**, page 4-3
  - **About the CallManager Administration Utility**, page 4-4
  - **How to Configure Agent IP Phones for IPCC Enterprise**, page 4-4
  - **How to Configure CTI Route Points**, page 4-6
  - **How to Configure CTI Ports**, page 4-7
  - **How to Configure JTAPI Users for the JTAPI Phones, CallManager PG and IP IVR**, page 4-7

**Note**

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

**Related Documentation**

The following additional Cisco documents provide additional information on the installation/configuration tasks described in this chapter:

- *Installing Cisco CallManager Guide*
- *Cisco CallManager Administration Guide*
- *Bulk Administration Tool Guide for Cisco CallManager*
- *Cisco CallManager Features and Service Guide*
- *Cisco Internet Service Node Configuration and Administration Guide*
About Cisco CallManager

CallManager provides features for which organizations have traditionally used PBX systems. CallManager uses open standards, such as TCP/IP, H.323 standards (for packet-based multimedia communications systems), and Media Gateway Control Protocol (MGCP). CallManager allows deployment of voice applications and the integration of telephony systems with Intranet applications. The CallManager software must be installed on the Cisco Media Convergence Server (MCS).

CallManager takes care of the switching requirements of the IPCC system. It uses Microsoft Internet Information Server (IIS) to allow remote administration with a standard Web browser, and it provides the basic services required for IP telephones, such as mapping IP addresses to specific devices and extensions, and managing Cisco Voice Gateways.

CallManager supports the Java Telephony Application Programming Interface (JTAPI) for deploying Cisco IP-IVR and other applications. Telephony applications written to the JTAPI specification can gain the cross-platform benefits of Java.

How to Install Cisco CallManager for IPCC Enterprise

Follow the step-by-step installation instructions for Cisco CallManager included in the Installing Cisco CallManager Guide. There are no IPCC-specific installation prerequisites or instructions for CallManager.

Once installation is complete, configure CallManager for IPCC as described in the next section. Prior to proceeding with configuration, ensure that:

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

Installing Cisco CallManager Guide
Bulk Administration Tool Guide for Cisco CallManager
# How to Configure CallManager for IPCC Enterprise

After installation, complete the tasks described in the following table to configure CallManager for use in an IPCC Enterprise Environment. These tasks should be performed in the order listed. Instructions for each are included later in this section.

<table>
<thead>
<tr>
<th>CallManager Configuration Tasks</th>
<th>Notes</th>
<th>Done?</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>
<td></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 Call Manager. The Route Points for dialed numbers must still be created in CallManager Administration.</td>
<td></td>
</tr>
<tr>
<td>3. Configure the CTI Ports</td>
<td>Only necessary for IP IVR deployments. Note: If you are using IP IVR 4.0(x) or later, CTI Ports can be configured directly in the IP IVR Administration interface.</td>
<td></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 CallManager PG, 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>
<td></td>
</tr>
</tbody>
</table>
About the CallManager Administration Utility

Most of the tasks in this chapter are performed from the CallManager Administration utility. CallManager Administration is installed on all CallManager. To access CallManager Administration, select Start > Programs > Cisco CallManager > Administration. Or, in a Web browser, enter http://<callmanagerservername>/ccmadmin.

How to Configure Agent IP Phones for IPCC Enterprise

How to Configure Agent IP Phones on the CallManager

To function with Cisco CallManager, each Cisco IP phone in your IPCC Enterprise system must be registered and configured with the CallManager Administration database. There are three different methods for doing this:

a. Manual configuration. In manual configuration, each agent IP phone is configured individually. This is the configuration method described in this chapter.

b. 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.
c. **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:

1. In CallManager Administration, select **Device > Add a Device.**
2. From Device Type, select **Phone.** Click **Next.**
3. From Phone Type, select the model of Cisco IP phone you are configuring. Click **Next.**
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.**
5. From Device Pool, select **Default.**
6. Click **Insert.** A message displays asking if you want to add a directory number for line 1 of this phone now. Click **OK.**
7. In Directory Number, enter the directory number for this phone. This will the agent’s ID for logging into the phone.
8. Click **Insert.** A message displays confirming the device record has been created in the CallManager database. Click **OK.**
9. 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:

1. Press **Settings.**
2. Press *** to unlock the configuration.
3. Select **Settings > Network Configuration > Select.**
4. Set Alternative TFTP to **Yes.**
5. Press **Save** and then press **Exit.**
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**

Cisco 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 CallManager PG.

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 PG is down or the IPCC cannot route a call, you can post-route the call to another CTI Route Point. Once a CTI Route Point has been created, lines (directory numbers) can be added and configured.

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:

1. In CallManager Administration, select Device > Add New Device.
2. From Device Type, select CTI Route Point. Click Next.
3. In Device Name, enter the Route Point name. Record the CTI Route Point Device Name. You will need this information when you configure a CTI Route Point on the IP IVR (described in Chapter 5, “Installing and Configuring Cisco IP IVR for IPCC Enterprise”) and configure a Dial Number on the ICM software (Chapter 6, “Installing and Configuring Cisco ICM for IPCC Enterprise”).
4. In Description, enter the service with which this CTI Route Point is associated.
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 the number of this device.
8. 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 ICM cannot route the call.
9. Click Insert.
10. Verify the CTI Route Point when finished by viewing the CTI Route Point Configuration fields.
11. Repeat this procedure to create additional CTI Route Points as needed. For example, you might create two route points for inbound dialing (one for post routing and one for translation routing) and two for IP IVR (one for post routing and one for transfer to IVR).
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 the IP IVR. Note that CTI ports are only necessary if you are deploying IP IVR in your IPCC Enterprise system.

The number of ports you configure is determined by your needs and available licenses.

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.
   Note
   Record the CTI Port Device Name that you enter. You need to configure a CTI Port on the IP IVR with this value.
5. In Description, enter the device name preceded by “Post Route Port.”
6. From Device Pool, select Default.
7. Click Insert. A message displays confirming the device record has been created in the CallManager database. Click OK.
8. In Directory Number, enter the same device name that you entered earlier.
9. Click Insert. A message displays confirming the directory number has been assigned to the current device. Click OK.
10. Repeat these steps to add additional route points, as necessary.

How to Configure JTAPI Users for the JTAPI Phones, CallManager PG 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 ICM software (the CallManager PG), and 2) the connection to the IP IVR (if you are deploying IP IVR).

Note

If you are using IP IVR 4.0(x) or later, the JTAPI user for IP IVR can be created directly in the IP IVR Administration interface; you do not need to configure them in CallManager. You must still create the JTAPI user for the CallManager PG in CallManager Administration.
How to Configure CallManager for IPCC Enterprise

**Note**

Instructions for installing the JTAPI Client on the CallManager PG follow later in Chapter 6, “Installing and Configuring Cisco ICM for IPCC Enterprise.”

**Note**

The following step-by-step instructions apply as-is for Cisco CallManager 4.x. For Cisco CallManager 5.x, however, you must first add an application user by choosing **User Management > Application User**
then add the user to the user group by choosing **User Management > User Group > Standard CTI Enable**

To configure JTAPI users for the CallManager PG and IP IVR:

1. In CallManager Administration, select **User > Add a New User**.
2. Enter a first and last name for the user.
3. In UserID, enter the User ID for the CallManager PG user.
4. In User Password, enter a password. Re-enter it in Confirm Password.
5. In PIN, enter an IP phone password (at least five characters). Re-enter it in Confirm PIN. You cannot leave this field blank.

**Note** Record the user names and passwords that you create for the JTAPI users for the CallManager PG and IP IVR. You need to configure a JTAPI user for the PG with the CallManager PIM in ICM Setup and on the IP IVR with these user names and passwords.

6. Select **Enable CTI Application Use**.
7. Click **Insert**.
8. Under Application Profiles, click **Device Association**.
9. Click **Select Devices**. All the Device names and extensions display.
10. Select all of the devices this user should control.
    - For the CallManager PG user, select the IP phones and the CallManager PG Route Points.
    - For the IP IVR PG user, select the Route Points for IP IVR Route Points and the Ports.
11. Select the **No Primary Extension** radio button.
12. Click **Update**.
13. Repeat these steps to create any additional CallManager PG users and an IP IVR PG user for each IP IVR system.
CHAPTER 5

Installing and Configuring Cisco IP IVR for IPCC Enterprise

This chapter describes how to install and configure Cisco IP IVR for the IPCC Enterprise in both production and laboratory environments. Follow the instructions in this chapter if you are using IP IVR (as opposed to CVP) for queuing in your IPCC system. (If you are deploying CVP instead of IP IVR, refer to Chapter 8, “Installing and Configuring Cisco CVP for IPCC Enterprise.”)

**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.

It contains these sections:
- About IP IVR, page 5-2
- How to Install IP IVR for IPCC Enterprise, page 5-2
  - About IP IVR Installation Prerequisites, page 5-3
- How to Configure IP IVR for IPCC Enterprise, page 5-3
  - How to Configure the Directory Profile, page 5-4
  - How to Configure the JTAPI User on the IP IVR System, page 5-6
  - How to Configure CTI Port Groups, page 5-6
  - How to Configure the ICM Subsystem, page 5-7
  - How to Configure and Upload VRU Scripts, page 5-9
  - About Translation Routing and Post Routing, page 5-9
  - How to Configure IP IVR for ICM Translation Routing, page 5-10
  - How to Configure IP IVR for ICM Post Routing, page 5-11
  - How to Configure and Start the Application Engine, page 5-12
  - How to Verify and Update the JTAPI Client, page 5-12
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.

Related Documentation
The following additional Cisco documents provide additional information on the installation/configuration tasks described in this chapter:

* Getting Started with Cisco Customer Response Applications Guide
* Cisco Customer Response Application Administration Guide

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.

IP-IVR automates the handling of calls by autonomously interacting with users. IP-IVR processes user commands to facilitate command response features such as access to checking account information or user-directed contact routing. IP-IVR also performs prompt and collect functions to obtain user data such as passwords or account identification. Cisco IP-IVR supports Open Database Connectivity (ODBC) access to Microsoft SQL Server, Oracle, Sybase, and IBM DB2 databases.

You can use IP-IVR to extract and parse Web-based content and present the data to customers using a telephony or HTTP interface.

IP-IVR communicates with ICM software by way of the Service Control Interface (SCI) protocol.

How to Install IP IVR for IPCC Enterprise
Step-by-step installation instructions for IP IVR are included in the *Getting Started with Cisco Customer Response Applications Guide*.

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 ICM 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*, page 5-12 for instructions.
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, you must:

<table>
<thead>
<tr>
<th>IP IVR Installation Prerequisite</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install and configure Cisco CallManager</td>
<td>On the CallManager configuration, you must have:</td>
</tr>
<tr>
<td></td>
<td>• Configured one CTI Route Point for each post route number and/or one for each translation route DNIS.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

Once installation is complete, configure IP IVR for IPCC as described in the next section. Prior to proceeding with configuration, ensure that:

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

How to Configure IP IVR for IPCC Enterprise

After installation, complete the tasks described in the following table to configure IP IVR for use in an IPCC Enterprise Environment. These tasks should be performed 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>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Configure JTAPI user on the IP IVR.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Configure CTI Port Groups.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Configure the ICM subsystem.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 5      Installing and Configuring Cisco IP IVR for IPCC Enterprise

How to Configure IP IVR for IPCC Enterprise

About the CRA Administration Utility

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

How to Configure the Directory Profile

You must enable the ICM subsystem on the IP IVR and 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: Configuration Directory and Repository.

The ICM subsystem of the IP IVR system allows the IP IVR to interact with the ICM software. The ICM Service Control interface allows the ICM software to provide call processing instructions to the IP IVR system. It also provides ICM software with event reports indicating changes in call state.

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 checkbox for the use a different repository profile option, multiple IP IVR directory profiles can share one easily updated repository. The repository keeps

### IP IVR Configuration Task

<table>
<thead>
<tr>
<th>IP IVR Configuration Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Create and upload VRU scripts.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Configure IP IVR for ICM Post / Translation Routing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Configure and start the Application Engine</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**About the CRA Administration Utility**

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

**How to Configure the Directory Profile**

You must enable the ICM subsystem on the IP IVR and 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: Configuration Directory and Repository.

The ICM subsystem of the IP IVR system allows the IP IVR to interact with the ICM software. The ICM Service Control interface allows the ICM software to provide call processing instructions to the IP IVR system. It also provides ICM software with event reports indicating changes in call state.

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 checkbox 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 CRA 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 CRA Engine profile. This information should be consistent with that entered in the CTI Manager A area on the CTI Manager Locations pane during CRA 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 should be consistent with the information entered in the CTI Manager B area on the CTI Manager Locations pane during CRA 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 CRA Administrator/Supervisor list box.
How to Configure IP IVR for IPCC Enterprise

Chapter 5  Installing and Configuring Cisco IP IVR for IPCC Enterprise

Step 16  For each user moved to the CRA 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 CRA 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 (you must configure one JTAPI user for each IP IVR in your system). This user must now be specified in the IP IVR configuration.

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:

1. In CRA Administration, select Subsystems > JTAPI.
2. In the JTAPI provider(s) field, enter your CallManager’s host name or ip address.
3. In the UserID and password fields, enter the information that you created in Cisco CallManager for the IP IVR user.

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.

4. Click Update.

How to Configure CTI Port Groups

A CTI Port Group is a group of access points into the IPCC telephone network. 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.

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 a Cisco ICM trunk group.

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 9002, the rest of the ports will be 9002 through 9020. With twenty ports, the IP IVR can handle twenty calls at a time.

If you are deploying your IPCC Enterprise system with multiple IP IVRs, note that each CTI Port Group must have a unique Group ID across all IP IVRs configured in the IPCC Enterprise system.
If your IPCC Enterprise deployment will use the System PG, your CTI Port Group IDs must: A) be an odd number, and B) be unique for all IP IVRs handled by a System PG. For example, if a System PG handles multiple IP IVRs and each IP IVR one CTI Port Group, then the CTI Port Group ID for the first IP IVR should be 1, the port group ID for the second IP IVR should be 3, and so on.

Caution

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.

Note

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.

To configure a CTI port group:

1. In CRA Administration, select Subsystems > JTAPI.
2. Click CTI Port Groups.
3. Click Add a New JTAPI Call Control Group.
4. In Group ID field, accept the automatic group ID, or enter a group ID. The Group ID corresponds to the trunk group number reported to the Intelligent Contact Management (ICM).
5. Press the Tab key to automatically populate the Description field.
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.
7. Click Associate CTI Ports.
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.
9. Select the check box(es) in the row that contains the directory number(s) of the CTI port.
10. Click Update.
11. Click Add.
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 of the IP IVR system allows the IP IVR system to interact with ICM software. ICM software provides a central control system that directs calls to various human and automated systems. ICM routing scripts can direct calls based on various criteria, such as time of day or the availability of subsystems.
The ICM subsystem is the queuing engine for IPCC Enterprise, which includes IP IVR. The ICM routing scripts can use four commands to interact with the IP IVR system:

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

In post-routing, the IP IVR system receives a call directly from Cisco CallManager, which sends the call to the post-routing route point on the IP IVR system. The IP IVR system searches the designated port group for a free CTI port and accepts the call.

If you configured this route point to run an initial application, such as a VRU script to welcome the caller and collect an account number, the IP-IVR system runs that script, notifies the ICM software about the call, and waits for further instructions. If you did not configure an initial application, the IP-IVR system just informs ICM software. ICM software runs a routing script after being notified of the call. ICM routing scripts are composed of many different call-handling steps. The IP-IVR system responds to the commands from ICM software until it signals that the call is complete. For example, the ICM routing script could send a Run VRU Script request to the IP-IVR system, instructing the IP-IVR system to run a VRU script that plays music and thanks the caller for their patience. When an agent becomes available, ICM software sends a Cancel request and the IP-IVR system stops running the current VRU script. ICM software 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.

To configure the ICM subsystem:

1. In CRA Administration, select **Subsystems > ICM**.
2. In the VRU Connection Port field, enter the same number that you will use when configuring the VRU peripheral interface manager (PIM) on the Cisco ICM system. The system uses this TCP/IP socket number for receiving messages from the Cisco ICM system.

   The default value in the Cisco ICM setup is 5000. Leave the default value unless you are configuring more than one VRU on the same PG. In that case, you have to assign a connection port for each VRU.

   **Note** Record the VRU Connection Port that you enter. You need to configure the VRU PIM on the ICM system with this value.

3. In the Service Control field, click the **Yes** radio button. The Service Control interface allows Cisco ICM to provide call-processing instructions to the IP IVR system. 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.
4. In the Parameter Separator field, enter the character used to delineate individual parameters in a multiple parameter variable.
5. In the Additional VRU Call Information check boxes, check any expanded call variables you want to use to pass call-related information.
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 CRA Engine.

IVR comes with some default scripts that are loaded as applications on the CRA Engine. You also can create your own VRU scripts using the Cisco CRA Editor. When configuring ICM software, 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 the ICM software sends a Run VRU Scripts request to the IP IVR system.

To configure ICM VRU Scripts.

1. In CRA Administration, select Subsystems > ICM.
2. Click ICM VRU Scripts.
3. Click Add a New VRU Script.
4. In the VRU Script Name field, enter a name for the VRU script you want to add.
5. In the Script field:
   - From the Script drop-down list, choose the CRA 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 ICM system with this value.

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.
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 translation routing and possibly post routing as well.

About 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.
About Post Routing

In post routing, IP IVR receives calls directly from Call Manager. Call Manager 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.

How to Configure IP IVR for IPCC Enterprise

- Cancel cancels the VRU script that is currently running.

How to Configure IP IVR for ICM 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 an IPCC routing application, you must first upload any VRU scripts that the application will need.

To configure IP IVR for ICM translation routing:

1. In CRA Administration, select Applications > Configure Applications.
2. Click Add a New Application.
3. From Application Type, select Cisco ICM Translation-Routing.
4. In the Name field, enter the name of the script on which the ICM translation-routing is based.
5. Press the Tab key to automatically populate the Description field.
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.
7. In Maximum Number of Sessions, enter the maximum number of sessions that the application will be able to handle simultaneously.
8. In the Enabled field, accept the default radio button Yes.
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.
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.
11. Click Add. A message displays confirming the operation has been successfully executed.
12. Click OK.
14. From Trigger Type, select JTAPI, and then click Next.
15. From CTI Route Point Directory Number, choose the CTI route point number that you configured in the Cisco CallManager.
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.
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.
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.
19. In the Enabled field, accept the default radio button Yes.
20. From the Call Control Group drop-down list, choose the appropriate call control group.
21. From the Primary Dialog Group drop-down list, choose the appropriate primary dialog group, or none.
22. From the Secondary Dialog Group drop-down list, choose the appropriate secondary dialog group, or none.
23. Click Add.

How to Configure IP IVR for ICM 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 ICM post routing:
1. In CRA Administration, select Applications > Configure Applications.
2. Click Add a New Application.
3. From Application Type, select Cisco ICM Post-Routing.
4. In the Name field, enter the name of the script on which the ICM translation-routing is based.
5. Press the Tab key to automatically populate the Description field.
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.
7. In Maximum Number of Sessions, enter the maximum number of sessions that the application will be able to handle simultaneously.
8. In the Enabled field, accept the default radio button Yes.
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.
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.
11. Click Add. A message displays confirming the operation has been successfully executed.
12. Click OK.
14. From Trigger Type, select JTAPI, and then click Next.
15. From CTI Route Point Directory Number, choose the CTI route point number that you configured in the Cisco CallManager.
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.
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.
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.
19. In the Enabled field, accept the default radio button Yes.
20. From the Call Control Group drop-down list, choose the appropriate call control group.
21. From the Primary Dialog Group drop-down list, choose the appropriate primary dialog group, or none.
22. From the Secondary Dialog Group drop-down list, choose the appropriate secondary dialog group, or none.
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.

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

To configure and start the Application Engine:
1. In CRA Administration, select System > Engine. (Note: System >Control Center in IP IVR 4.0(x)).
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.
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 Cisco Call Manager server and installs this JTAPI Client on the server.

If you change versions of Cisco CallManager after installing IP IVR, Cisco 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 CRA 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 CRA Administration.
This chapter describes how to install and configure Cisco ICM software for the IPCC Enterprise system. It contains these sections:

- About Cisco Intelligent Contact Management Software, page 6-2
  - About ICM Components, page 6-2
- How to Install ICM for IPCC Enterprise, page 6-2
  - How to Enable ICM Outbound Option During ICM Installation, page 6-3
  - About ICM Installation Prerequisites, page 6-3
- How to Configure ICM for IPCC Enterprise, page 6-3
  - About ICM Configuration Tasks, page 6-3
  - About the ICM Bulk Configuration Tool, page 6-5
  - How to Configure Agent Desk Settings, page 6-6
  - How to Create a Network VRU, page 6-9
  - How to Configure and Install the System PG, page 6-10
  - How to Configure and Install the Generic PG, page 6-15
  - How to Install the Cisco JTAPI Client on the System or Generic PG, page 6-21
  - How to Configure and Install the Media Routing PG, page 6-22
  - How to Configure Trunk Groups, page 6-24
  - How to Configure the Network VRU Bank, page 6-26
  - How to Configure Services, page 6-26
  - How to Configure Skill Groups, page 6-27
  - How to Configure Persons, page 6-30
  - How to Configure Agents, page 6-31
  - How to Configure Dialed Numbers, page 6-35
  - How to Configure Routes, page 6-35
  - How to Configure Device Targets, page 6-36
  - How to Configure Labels, page 6-37
About Cisco Intelligent Contact Management Software

As part of IPCC, Cisco ICM software provides ACD functionality including monitoring and control of Agent State, routing and queuing of contacts, CTI capabilities, real-time data for agents and supervisors, and gathering real-time and historical data for reporting in the IPCC Enterprise system.

The basic ICM software includes the following components: CallRouter, Logger, Peripheral Gateway, CTI Server, and Admin Workstation.

About ICM Components

Before you can configure ICM for use in an IPCC Enterprise environment, you must first install the following ICM software components:

<table>
<thead>
<tr>
<th>ICM Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Workstation</td>
<td>The Admin Workstation is the human interface to the ICM software. You use the Admin Workstation to monitor activity in the IPCC Enterprise system and modify configuration data and routing scripts.</td>
</tr>
<tr>
<td>CallRouter</td>
<td>The CallRouter is the Central Controller component of ICM software. The CallRouter executes routing scripts to determine the destination of each call. It also gathers data from the Peripheral Gateways and distributes monitoring data to the Admin Workstation.</td>
</tr>
<tr>
<td>Logger</td>
<td>The Logger is the ICM software component that stores the central ICM database.</td>
</tr>
<tr>
<td>Historical Data Server (HDS) Databases</td>
<td>You install a Historical Data Server Database on each Logger.</td>
</tr>
<tr>
<td>CTI Server</td>
<td>The CTI Server is the ICM software component that provides an interface between the agent desktops and the PG for CallManager.</td>
</tr>
</tbody>
</table>

How to Install ICM for IPCC Enterprise

Step-by-step installation instructions for ICM are included in the ICM Software Installation Guide. When installing ICM for use in an IPCC Enterprise system:

- When installing the AW and Logger, if you will be deploying the Outbound Option feature, enable Outbound Option as described in How to Enable ICM Outbound Option During ICM Installation, page 6-3.
How to Enable ICM Outbound Option During ICM Installation

Outbound Option is an ICM feature that allows agents to make automatic outbound calls to customers. To enable this feature, certain settings must be chosen when ICM components are installed. For more information, see Chapter 7, “Installing and Configuring Outbound Option for IPCC Enterprise” or the Outbound Option Setup and Configuration Guide for Cisco ICM/IPCC Enterprise & IPCC Hosted Editions.

About ICM Installation Prerequisites

Before installing and configuring ICM for use with IPCC enterprise, you must:

<table>
<thead>
<tr>
<th>ICM Installation Prerequisite</th>
<th>Installation/Configuration Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Cisco CallManager</td>
<td>On the CallManager, you must have:</td>
</tr>
<tr>
<td></td>
<td>• Configured one CTI Route Point for each post route number and/or one for each translation route DNIS.</td>
</tr>
<tr>
<td></td>
<td>• Created a CallManager PG user and associated the user with CTI Route Point(s) and CTI Port(s).</td>
</tr>
<tr>
<td></td>
<td>• Enabled CTI for the CallManager PG user.</td>
</tr>
<tr>
<td>Install IP IVR if your IPCC Enterprise system will use IP IVR for queueing</td>
<td>On the IP IVR, you must have:</td>
</tr>
<tr>
<td></td>
<td>• Configured the VRU Port Group.</td>
</tr>
<tr>
<td></td>
<td>• Configured the ICM subsystem.</td>
</tr>
<tr>
<td></td>
<td>• Uploaded VRU scripts.</td>
</tr>
<tr>
<td></td>
<td>• Specified the VRU Connection Port.</td>
</tr>
<tr>
<td></td>
<td>• Configured translation routing on the IP IVR.</td>
</tr>
</tbody>
</table>

How to Configure ICM for IPCC Enterprise

After installation, complete the tasks described in this section to configure ICM for use in an IPCC Enterprise Environment.

About ICM Configuration Tasks

The following table lists the configuration tasks required to ICM in an IPCC Enterprise deployment. These tasks should be performed in the order listed. Instructions for each are included later in this section.

<table>
<thead>
<tr>
<th>ICM Configuration Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure agent desk settings.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Configure a Network VRU.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### ICM Configuration Task

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Configure and install either the System PG or the Generic PG.</td>
<td>You must configure the PG before installing it. Generally speaking, you would use the: System PG if you are deploying IP IVR. Generic PG if you are deploying CVP.</td>
<td></td>
</tr>
<tr>
<td>4. Install the JTAPI Client on the PG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Configure and install the MR PG</td>
<td>You create MR PGs only if you are deploying Outbound Option or the Multichannel options. You must configure the MR PG before installing it.</td>
<td></td>
</tr>
<tr>
<td>6. Configure network trunk groups.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Configure trunk groups.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Configure the Network VRU Bank.</td>
<td>For System PG deployments only.</td>
<td></td>
</tr>
<tr>
<td>9. Configure services.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Configure skill groups.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Configure persons.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Configure agents.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. Configure routes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14. Configure dialed numbers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17. Configure call types.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18. Configure dialed number plan.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20. Configure VRU scripts.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21. Configure routing and administrative scripts.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
About the ICM Configuration Manager

All of the tasks in this chapter are performed from the ICM Configuration Manager. The ICM Configuration Manager is installed on all ICM Admin Workstations. To access the ICM Configuration Manager, select Start > Programs > ICM > Admin Workstation > Configuration Manager.

About the ICM Bulk Configuration Tool

You can use the ICM Configuration Manager Bulk Configuration Tool to insert and update multiple configuration records in a single transaction.

To access the Bulk Configuration Tool, in the ICM Configuration Manager select Tools > Bulk Configuration.

The Bulk Configuration Tool lets you to configure the following in bulk:

- Persons
- Agents
- Call Types
- Dialed Number Plans
- Device Targets
- Labels
- Network Trunk Groups
- Network VRU Scripts
- Peripheral Targets
- Routes
- Services
How to Configure Agent Desk Settings

Agent Desk Settings associate a set of permissions or characteristics with specific agents. The settings are comparable to Class of Service settings on a PBX or ACD. Desk settings are associated with an agent when the agent is configured. The desk settings are global in scope and they can be applied to any configured agent on any peripheral within an ICM configuration.

If Agent Desk Settings are not associated with an agent, the agent is assigned the peripheral default settings, which depend on the peripheral to which the agent is assigned.

When you configure Agent Desk Settings, you specify the amount of non-active time after which an agent is automatically logged out, whether wrap up is required following incoming and outbound calls, the amount of time allocated for wrap up, and the method used for assist and emergency calls. You also specify settings for the Re-route on No Answer feature.

This section contains:
- About Re-route on No Answer, page 6-6
- How to Configure Agent Desk Settings, page 6-8

About Re-route on No Answer

The Re-route on No Answer feature, configured in Agent Desk Settings, ensures that when an agent does not answer a call, the call is taken away from the agent after a specified number of seconds and re-assigned to another agent or requeued.

This feature behaves and is configured differently depending on whether you have deployed CVP or IP IVR in the IPCC Enterprise System.

Note

The Dialed Number for Re-route On No Answer is peripheral-specific. Therefore, each CallManager PG in your deployment must have its own set of Agent Desk Settings configured for it; you cannot use a particular desk setting across peripherals.

This section provides the following information about the Re-route on No Answer feature:
- About Re-route on Ring No Answer with IP IVR, page 6-6
- About Re-route on No Answer with CVP, page 6-7

About Re-route on Ring No Answer with IP IVR

For IPCC Enterprise systems in which IP IVR is deployed, the Re-route on Ring No Answer feature ensures that when an agent does not answer a call:
- The call is taken away from that agent after ringing for a configurable number of seconds and is re-routed to a different agent or placed in queue.
- The state of the agent who did not answer the call is changed to “Not Ready”.
Re-route a call on Ring No Answer works as follows for IP IVR:

1. A routing script connects the call to an agent.
2. If the agent does not answer the phone within the Ring No Answer time set in Agent Desk Settings, the CallManager changes the agent’s state to “Not Ready” and post-routes the call to the ICM.
3. The ICM Router runs a routing script using the dialed number specified in the agent desk setting record. The routing script associated with the DN typically looks for another agent and routes the call to that new agent.
4. If no agents are available, the call typically is translation-routed or queued to the IVR, or sent to some other queue point. Queuing treatment is restarted.

Note: That call should be given the highest priority in the queue so that the call is routed to the next available agent.

5. Any call data is preserved to be popped onto the agent screen. In addition, a flag is set in the database so that ICM software can report on all of the occurrences of Re-route on Ring No Answer. (WebView provides historical reports for both the agent and skill group that contain a Redirect No Answer field. This field increments every time a call is redirected off the agent’s desk for the skill group related to the call.)

About Re-route on No Answer with CVP

For IPCC Enterprise systems in which CVP is deployed, the Cisco CallManager does not control the CVP and cannot send an unanswered call back to the CVP for re-queueing. You configure the Re-route on No Answer feature to only make the agent “Not Ready” when he/she does not answer a call, and use the CVP Router Requery feature to re-queue the call.

Re-route a call on Ring No Answer works as follows for CVP:

1. A routing script connects the call to an agent by sending a connect message to the CVP (the script node has “Requery” enabled”)
2. The agent’s phone rings.
3. If the phone is not answered (either via the agent desktop or physically going off-hook) within the Ring No Answer time set in Agent Desk Settings, the ICM makes the agent unavailable, but does not actually change the agent state to Not Ready until the call is re-directed.
4. When the CVP Ring No Answer timeout expires, the CVP sends an EventReport=No Answer message to the router instructing it to select another target according to the routing script and send a Connect message to the CVP. The target may be another agent or a VRU label to requeue the call.

Note: That call should be given the highest priority in the queue so that the call is routed to the next available agent.

5. Any call data is preserved to be popped onto the second agent screen.

Note: In addition, a flag is set in the database so that ICM software can report on all of the occurrences of Re-route on Ring No Answer. (WebView provides historical reports for both the agent and skill group that contain a Redirect No Answer field. This field increments every time a call is redirected off the agent’s desk for the skill group related to the call.)
6. When the call is redirected from the original agent, the agent’s state changes to Not Ready.

How to Configure Agent Desk Settings

To configure Agent Desk Settings:

1. From the ICM Configuration Manager, choose Configure ICM > Enterprise > Agent Desk Settings List. The ICM Agent Desk Settings List dialog box opens.
2. Click Retrieve.
3. Click Add.
4. Fill in the Attributes tab information:
   - **Name.** Enter a name for the agent desk settings that is unique within the enterprise.
   - **Ring No Answer Time.** Enter the number of seconds (between 1 and 120) that a call may ring at the agent’s station. If you are deploying CVP, this number should be less than the number set for the No Answer Timeout for Router Requery that you set in CVP.
     
     If you configure this timer, you do not need to configure CallManager’s Call Forward on No Answer for agent extensions in CallManager, unless you want them to be used when the agent is not logged in. If you set the CallManager Call Forward No Answer time, enter a value at least 3 seconds higher than the ICM Ring No Answer Time on each CallManager node.
   - **Ring No Answer Number.** Enter the ICM DN associated with the ICM routing script that you want to use to re-route a call that an agent has not answered. If you are deploying CVP, leave this field blank.
   - **Logout non-activity Time.** Enter the number of seconds (between 10 and 7200) in which the agent can remain in Not Ready state before ICM software automatically logs out the agent.
   - **Work Mode on Incoming.** Select whether wrap-up is required following an incoming call. Select an option from the drop-down list.
   - **Work Mode on Outgoing.** Select whether wrap-up is required following an outgoing call. Select an option from the drop-down list.
   - **Wrap Up Time.** Enter the amount of time, in seconds, allocated to an agent to wrap up a call.
   - **Assist Call Method.** Select whether IPCC will create a consultative call or a blind conference call for a supervisor assistance request.
   - **Emergency Alert Method.** Select whether IPCC will create a consultative call or a blind conference call for an emergency call request.

   **Note** Blind conference is not supported if the call may queue on an IVR.

   - **Description.** Enter additional optional information about the agent desk settings.
5. Use the following boxes to select or de-select miscellaneous settings:
   - **Auto-answer.** Indicates whether calls to the agent are automatically answered. The agent is not required to take any action to answer the call.
   - **Idle Reason Required.** Indicates whether an agent is required to enter a reason before entering the Idle state.
   - **Logout Reason Required.** Indicates whether an agent is required to enter a reason before logging out.
**AutoRecord on Emergency.** Indicates in a record request is automatically sent when an emergency call request starts.

6. Use the following boxes to select or de-select the Outbound Access settings:
   - **International.** Indicates whether agents are allowed to initiate international calls.
   - **National.** Indicates whether agents are allowed to initiate calls through the local private network.
   - **Local Private Network.** Indicates whether agents are allowed to initiate calls through the local private network.
   - **Operator Assisted.** Indicates whether agents are allowed to initiate operator assisted calls.
   - **PBX.** Indicates whether agents are allowed to initiate outbound PBX calls.

The Call Types for outbound calls are configured using the Number Plan configuration tabs. See the Configuring Call Types section for more information.

7. Click **Save** and then click **Close**.

**How to Create a Network VRU**

Configuring a Network VRU is part of setting up queueing in your IPCC Enterprise system. A VRU is a telecommunications computer that responds to caller-entered digits. A Network VRU supports the ICM’s service control interface. An ICM routing script can divert a call to a Network IVR (CVP or IP IVR) and instruct the IVR to perform specific processing before the ICM determines the final destination for the call. Each routing client can have one or more associated VRUs.

Setting up a Network VRU involves:

- Creating a Network VRU target for each VRU type deployed in your system.
- If you are using CVP and/or are deploying IPCC Enterprise with the Generic PG, inserting IVR nodes in the routing script.

To create a Network VRU target:

1. In the ICM Configuration Manager, select **Targets > Network VRU > Network VRU Explorer.** The Network VRU Explorer dialog box opens.
2. Click **Retrieve.**
3. Click **Add Network VRU.**
4. On the Network VRU tab, add the following values:
   - **Name:** Add a suitable name.
   - **Type:** If you are deploying the System PG, choose type 9. If you are deploying IP IVR with the Generic PG, choose **Type 2.** If you are deploying CVP, the type you choose depends on your CVP deployment model. If you are creating the VRU target for an MR PG, choose Type 2.
5. Click **Save** and then click **Close**.

**About IPCC Peripheral Gateways**

In IPCC terms, a **Peripheral** is a switch such as an ACD or VRU that receives calls that have been routed by the IPCC central controller. A **Peripheral Gateway (PG)** is the physical hardware platform and the logical software process that runs on it that communicates with an ACD or VRU. The PG reads status...
information from the peripheral and communicates it to the IPCC central controller. PGs and peripherals communicate with one another via Peripheral Interface Managers (PIMs), the IPCC proprietary interface between PGs and peripherals.

To allow direct communication between the ICM software and the Cisco CallManager and IP IVR or CVP, you must configure peripherals and PGs for CallManager and the VRU(s). You configure peripherals as part of the Peripheral Gateway configuration. Agents are grouped together by peripheral for the purposes of reporting, call handling, and other administrative functions.

IPCC Enterprise 7.0(0) supports three basic types of peripheral gateways:

- The System PG is the easiest PG type to configure and maintain. It requires only a single peripheral to communicate with CallManager and IP IVR. It is also the only PG type that is supported in IPCC Gateway deployments, an architecture in which child IPCCs can communicate and route calls to and from a parent ICM. The System PG is not supported with CVP; it can be used with IP IVR only.

  **Note** This guide describes how to deploy IPCC Enterprise with the System PG. This is not to be confused with System IPCC Enterprise, a very different deployment model orderable from Cisco as a separate product.

- The Generic PG is a consolidated PG that requires both separate peripherals for CallManager and the VRU. While more difficult to configure than the System PG, it can support CVP.

- You can also install CallManager and VRU peripherals on separate physical PGs, individually referred to as the CallManager PG and the VRU PG.

You can install PG software on the same server as the ICM central controller or on a different server. If the PG is in a different domain than the Central Controller, you must set up a trust relationship between the domains.

**How to Configure and Install the System PG**

The System PG is the easiest PG type to configure and maintain. It requires only a single peripheral to communicate with CallManager and IP IVR. It is also the only PG type that is supported in IPCC Gateway deployments, an architecture in which child IPCCs can communicate and route calls to and from a parent ICM. The System PG is not supported with CVP; it can be used with IP IVR only.

Configuring and installing the System PG requires you complete the following tasks:

- How to Configure the System PG
- How to Configure the System PG Peripheral
- How to Install the System PG
- How to Install the Cisco JTAPI Client on the System or Generic PG

**How to Configure the System PG**

You must configure a PG before you can install it.

To configure the System PG:

1. In the ICM Configuration Manager, select Tools > Explorer Tools > PG Explorer.
2. Click Retrieve.
3. Click Add.
4. Complete the Logical Controller section as follows:
   - **Logical Controller ID**: Leave blank. This value will be auto-generated when the record is saved.
   - **Physical Controller ID**: Leave blank. This value will be auto-generated when the record is saved.
   - **Name**: Enter a unique enterprise name for the PG.
   - **Client Type**: Select IPCC System.
   - **Configuration Parameters**: Leave blank.
   - **Description**: As desired, enter any other information about the PG. ICM Configuration Manager copies this value to the description fields of the logical interface controller, physical interface controller, peripheral, and (if applicable) the routing client records.
   - **Physical Controller Description**: As desired, enter a description for the physical controller.

At this point, you are now ready to add the peripheral for the System PG.

**How to Configure the System PG Peripheral**

To configure the Peripheral for the System PG:

1. With the PG record open in the ICM Configuration Manager PG Explorer, highlight the PG icon in the tree hierarchy in the lower-left corner of the window. Click **Add Peripheral**.

2. On the Peripheral tab, enter the following:
   - **Name**: Enter a unique enterprise name for this peripheral.
   - **Peripheral Name**: Enter the name of the peripheral as it is known at the site. Unlike the Enterprise Name field, the value of this field does not have to be unique. For example, at each site you might label the peripherals Switch1, Switch2, and so forth.
   - **Client type**: Select IPCC System.
   - **Location**: Enter the peripheral's location. For example: the name of a city, building, or department.
   - **Abandoned Call Wait Time**: Enter the minimum time (in seconds) an incoming call must be queued before being considered an abandoned call if the caller hangs up.
   - **Configuration Parameters**: As desired, enter a string containing any parameters that must be sent to the device to initialize it. In most cases, you should leave this field blank.
   - **Call Control Variable Map**: As desired, enter a string that describes the mappings of the peripheral’s call control variables to ICM software’s call control variables.
   - **Description**: As desired, enter any additional information about the peripheral.
   - **Default Desk Settings**: Select the default desk settings for agents associated with the peripheral.
   - **Peripheral Service Level Type**: The default type of service level calculation to be performed by the peripheral for it associated services. Select “Calculated by CallCenter.”
   - **Enable Post Routing**: Check this box to enable the CallManager peripheral to send route requests to the ICM router. When you check this box, the Routing Client tab is enabled.

3. On the Advanced tab, enter the following:
   - **Available Holdoff Delay**: For IPCC, set this field to zero.
   - **Default Route**: The default route associated with this peripheral. Default routes are configured with the ICM Configuration Manager.
Answered Short Calls Threshold. Maximum duration, in seconds, for a short call. Any calls with a duration below the threshold are considered short. You might then choose to factor out short calls from handle times you calculate. Refer to the Cisco IP Contact Center Reporting Guide for more information on configuring short calls.

Network VRU. The type of network VRU. Select the Type 9 network VRU you created earlier.

Agent Auto-Configuration. Not an option for IPCC. Leave this option disabled.

Internal IPTA Only. For the System PG, this box should be checked.

When checked, agents on the PG can be targeted by that PG only—the router uses the skill group IPTA configuration to select agents. When unchecked, for calls routed between different PGs, the router picks the agent (which would largely undo the benefit of the System PG. Unchecking would also necessitate the creation of additional device targets.

4. On the Agent Distribution tab, enter the following:
   
   Enable Agent Reporting. Check to allow IPCC reporting on agents.

   Distributor Site Name. Click New and enter the site name of the Admin Workstation to which the ICM router and logger should send agent information. Note that the site name of the AW distributor is the same name that is entered during AW distributor set up. If nothing is entered for the site name during installation, it defaults to the host name. After specifying the AW, ensure the Enabled check box is selected.

   Agent Event Detail. Enables label text (as opposed to numeric) Not Ready Reason Code reporting.

5. On the Routing Client tab, enter the following:
   
   Name. An enterprise name for this routing client. The name must be unique among all routing clients in the enterprise.

   Timeout threshold. The maximum time, in milliseconds, the routing client can wait for a response to a routing request.

   Late threshold. The threshold value, in milliseconds, for classifying responses as late. Any response that exceeds this threshold is considered late even if it does not exceed the TimeoutThreshold.

   Timeout limit. The maximum time, in seconds, for which the routing client waits for a response. If the routing client receives no responses from the ICM system within this limit, it terminates routing operation.

   Default call type. The call type to be used for any route request that does not match a defined call type mapping. The drop-down list contains all configured call types.

   ICM software uses the default call type for any routing request from the routing client that does not otherwise map to a call type. If you do not define a default call type for the routing client, ICM software uses a general default call type if you define one through the System Information command.

   Configuration parameters. Leave blank for IPCC.

   Use DN/Label map. Indicates whether only specific labels are valid for each dialed number associated with this routing client (when selected) or whether all labels associated with the routing client are valid for any dialed number (when not selected). Leave unchecked for IPCC.

   Client type. Indicates the type of client. Select VRU.

   Description. Additional information about the routing client.
Network routing client. A name used to associate routing clients across instances.

Network transfer preferred. If checked, indicates that network transfer is preferred. When the target of a call is reachable by both a label defined for the requesting routing client and by another label defined for the network routing client that pre-routed the call, this option indicates which choice is preferred.

6. On the Default Route tab, select Cisco_Voice as the Media Routing Domain.
7. Click Save.
8. Once the record is saved, you can view the ID of a peripheral from the PG Explorer dialog. To view a peripheral record, start the PG Explorer from the Configuration Manager. The Logical controller ID is found on the Logical controller tab and the Peripheral ID displays on the Peripheral tab.

How to Install the System PG

After the System PG has been configured, you then install the PG software on the PG machine. Before installing the System PG, record the Logical controller ID and Peripheral ID for the PG (from the PG Explorer).

To install the System PG:
1. On the PG machine, from the ICM CD-ROM run setup.exe.
2. In the Instance Components section, select the ICM Instance to which you are adding the PG and click Add and choose Peripheral Gateway from the ICM Component Selection window.

Note If the ICM instance which you want to add the PG has not been defined on this machine yet, use setup to create it before proceeding with the PG install. See the ICM installation documentation for more information on setting up instances.

3. Choose Production Mode and Auto Start at System Startup unless you are specifically told otherwise by your Cisco Support representative. This ensures that the Peripheral Gateway can restart itself automatically if necessary.
4. Specify whether the PG is part of a duplexed pair.
5. In the ID field, choose the PG’s device identifier as enabled in the CallRouter’s DMP configuration dialog box.
6. In the Client Type sections, add IPCC System and VRU as the client types. Use the Add and Remove buttons to select or de-select PG types.
7. If the PG is duplexed, specify whether you are installing Side A or Side B. If the PG is simplex, select Side A.
8. Choose the local disk on which you want to install the PG software.
9. Choose the language.
10. Click Next. The Peripheral Gateway Component Properties window opens.
11. In the Peripheral Gateway Configuration section of the window, enter the Controller ID from the Logical_Interface_Controller record for the PG. The Controller ID is defined in ICM Configuration Manager when you configure the PG.
12. The next step is to add the peripheral interface managers (PIMs). You must add one (and only one) PIM for the IPCC System client type, and one PIM of client type VRU for each IP IVR in your deployment.
To add the IPCC System PIM:

a. Click Add. Select IPCC System from the Available PIMs list. The IPCC System Configuration dialog box opens.
b. To put the PIM into service, check the Enabled option. This allows the PIM to communicate with the peripheral when the Peripheral Gateway is running.
c. In the Peripheral name field, enter the Peripheral name of the parent server from the configuration Manager (use the PG Explorer tool to view the Peripheral name).
d. In the Peripheral ID field, from the Peripheral record, enter the Peripheral ID value from the Configuration Manager (use the PG Explorer tool to view the Peripheral ID).
e. In the Agent extension length field, enter the number of digits in the agent extension. The default is 7; the maximum is 15.
f. In the Service field, enter the host name or the IP address of the machine that is running the Cisco CallManager software. If using the host name, the name must be in the hosts file.
g. In the User ID field, enter the User ID entered for the PG on the Cisco CallManager Administrator web page when you added the PG as a new user. (This field cannot be blank.)
h. In the User password field, enter the User Password entered for the PG on the Cisco CallManager Administrator web page. (This field cannot be blank.)
i. Click OK.

To add the VRU PIM(s):

a. Click Add. Select VRU from the Available PIMs list. The VRU Configuration dialog box opens.
b. To put the PIM into service, check the Enabled option. This allows the PIM to communicate with the peripheral when the Peripheral Gateway is running.
c. In the Peripheral name field, enter the Peripheral name of the parent server from the configuration Manager (use the PG Explorer tool to view the Peripheral name).
d. Peripheral IDs for VRU PIMs are assigned automatically by Setup and are viewable only from the Windows registry. Values range sequentially from 4500-4999.
e. In the VRU host name field, enter the name by which the VRU is known to the network.
f. Enter the number of the VRU connection port that the PG connects to.
g. In the Reconnect interval (sec) field, specify how often, in seconds, the PG will try to re-establish a lost connection to the VRU. The default value is usually appropriate.
h. In the Heartbeat interval (sec) field, specify how often, in seconds, the PG will check its connection to the VRU. The default value is usually appropriate.
i. Click OK.

13. When you are done adding the PIMs, click Next. The Device Management Protocol Properties window displays.

14. If you prefer that the PG communicate with one side or the other of the Central Controller (for example, if the PG is collocated with one side), indicate the preferred side. Whether you specify a preferred side or not, if the PG cannot communicate with one side, it will automatically switch to the other.

15. Indicate whether the PG is local to or remote from each side of the Central Controller. If the PG is remote from either side, specify the maximum amount of bandwidth (in bits per second) the PG can use for communication with the CallRouter. Use this option to prevent the PG from overloading the wide-area network.
16. Indicate how often the PG should send heartbeats to the Central Controller. Specify the number of 100 millisecond intervals between heartbeats. For example, the default value of 4 means a heartbeat is sent every 400 milliseconds. The CallRouter considers the PG to be off-line if it misses five consecutive heartbeats. (By default, this occurs in two seconds.)

17. To configure the PG QoS settings, click Advanced. The PG QoS DMP Properties Advanced Options window displays.

18. Set the DSCP (DiffServ Codepoint) marking for each priority of the ICM traffic going to the Call Router. The defaults are acceptable if your network is Cisco AVVID compliant (Architecture for Voice, Video and Integrated Data). Otherwise, you need to consult your network administrator or Cisco representative for the proper values for these fields.

19. Uncheck the Bypass QoS packet scheduler box if you plan to use the Microsoft Packet Scheduler utility. This changes the appearance of the PG QoS DMP Properties Advanced Options window. The edit boxes for Medium Priority are grayed out and the Medium Priority always has the same settings as the High Priority. This is because Microsoft Packet Scheduler supports at most two classification levels (except best effort).

20. In addition to DSCP marking, the Class-of-Service (802.1p) marking is supported. The default values are set in compliance with Cisco AVVID recommendations. Consult your network administrator or Cisco representative for changes.

Note Microsoft Packet Scheduler must be installed separately from the ICM setup if you uncheck the Bypass Packet Scheduler box. For more information about QoS for the ICM software, refer to the Pre-Installation Planning Guide for Cisco ICM Enterprise Edition.


22. Click Next. The Peripheral Gateway Network Configuration window displays.

Enter the TCP/IP addresses or host name of the PG and, if it is duplexed, its pair. If the PG is simplex, enter localhost for the B side addresses. Also enter the visible network addresses for the CallRouter machines.

23. Click Next. The Check Setup Information window displays.

Ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the Back button. When the settings are correct, click Next to begin copying files.

24. Click Finish to exit Setup and optionally start the Node Manager.

How to Configure and Install the Generic PG

The IPCC Enterprise system offers a consolidated PG that houses both the CallManager and VRU peripherals, the Generic PG. You can install the PG software on the same server as the ICM central controller or on a different server. If the PG is in a different domain than the Central Controller, you must set up a trust relationship between the domains.

You create one CallManager peripheral per CallManager cluster and one VRU peripheral per IP IVR or CVP.

In general, you can configure 32 peripherals per PG. The actual number of peripherals that can run on one PG depends on loading factors, such as calls per second and the number of agents. The Cisco IP Contact Center Solution Reference Network Design Guide provides guidance for determining the number of peripherals and PGs required in your system.
Configuring and installing the Generic PG requires you complete the following tasks:

- How to Configure the Generic PG
- How to Configure the CallManager Peripheral
- How to Configure the VRU Peripheral
- How to Install the Generic PG
- How to Install the Cisco JTAPI Client on the System or Generic PG

### How to Configure the Generic PG

You must configure a PG before you can install it. At the time you configure a new PG, you must add at least one Peripheral to it or you will not be able to save the configuration.

To configure the Generic PG:

1. In the ICM Configuration Manager, select Tools > Explorer Tools > PG Explorer.
2. Click Retrieve.
3. Click Add.
4. Complete the Logical Controller section as follows:
   - **Logical Controller ID:** Leave blank. This value will be auto-generated when the record is saved.
   - **Physical Controller ID:** Leave blank. This value will be auto-generated when the record is saved.
   - **Name:** Enter a unique enterprise name for the PG.
   - **Client Type:** Select the PG Generic client type from the drop-down list. If you were installing a standalone CallManager PG (as opposed to the Generic PG) you would select CallManager/SoftACD.
   - **Configuration Parameters:** Leave blank.
   - **Description:** As desired, enter any other information about the PG. ICM Configuration Manager copies this value to the description fields of the logical interface controller, physical interface controller, peripheral, and (if applicable) the routing client records.
   - **Physical Controller Description:** As desired, enter a description for the physical controller.
   - **Primary CTI Address:** Enter the address for the primary CTI server. Make this entry in the form of `<an IP address or server name where the CTI server is installed>`: `<Client Connection Port Number>`. Secondary CTI Address: Enter an address for a secondary CTI server (for duplexed systems).

At this point, you are now ready to add the CallManager and VRU peripherals to your PG. Note that you will be unable to save the PG configuration you’ve entered thus far until you’ve added at least one peripheral.

### How to Configure the CallManager Peripheral

To configure a CallManager Peripheral:

1. With the PG record open in the ICM Configuration Manager PG Explorer, highlight the PG icon in the tree hierarchy in the lower-left corner of the window. Click Add Peripheral.
2. On the Peripheral tab, enter the following:
Name: Enter a unique enterprise name for this peripheral.

Peripheral Name: Enter the name of the peripheral as it is known at the site. Unlike the Enterprise Name field, the value of this field does not have to be unique. For example, at each site you might label the peripherals Switch1, Switch2, and so forth.

Client type: Select CallManager/SoftACD.

Location: Enter the peripheral's location. For example: the name of a city, building, or department.

Abandoned Call Wait Time: Enter the minimum time (in seconds) an incoming call must be queued before being considered an abandoned call if the caller hangs up.

Configuration Parameters: As desired, enter a string containing any parameters that must be sent to the device to initialize it. In most cases, you should leave this field blank.

Call Control Variable Map: As desired, enter a string that describes the mappings of the peripheral’s call control variables to ICM software’s call control variables.

Description: As desired, enter any additional information about the peripheral.

Default Desk Settings: Select the default desk settings for agents associated with the peripheral.

Peripheral Service Level Type: The default type of service level calculation to be performed by the peripheral for it associated services. Select “Calculated by CallCenter.”

Enable Post Routing: Check this box to enable the CallManager peripheral to send route requests to the ICM router. When you check this box, the Routing Client tab is enabled.

3. On the Advanced tab, enter the following:

Available Holdoff Delay: For IPCC, set this field to zero.

Default Route: The default route associated with this peripheral. Default routes are configured with the ICM Configuration Manager.

Answered Short Calls Threshold. Maximum duration, in seconds, for a short call. Any calls with a duration below the threshold are considered short. You might then choose to factor out short calls from handle times you calculate. Refer to the Cisco IP Contact Center Reporting Guide for more information on configuring short calls.

Network VRU. The type of network VRU. For the CallManager peripheral, select None.

Agent Auto-Configuration. Not an option for IPCC. Leave this option disabled.

4. On the Agent Distribution tab, enter the following:

Enable Agent Reporting. Check to allow IPCC reporting on agents.

Distributor Site Name. Click New and enter the site name of the Admin Workstation to which the ICM router and logger should send agent information. Note that the site name of the AW distributor is the same name that is entered during AW distributor set up. If nothing is entered for the site name during installation, it defaults to the host name. After specifying the AW, ensure the Enabled checkbox is selected.

Agent Event Detail. Enables label text (as opposed to numeric) Not Ready Reason Code reporting.

5. On the Routing Client tab, enter the following:

Name. An enterprise name for this routing client. The name must be unique among all routing clients in the enterprise.

Timeout threshold. The maximum time, in milliseconds, the routing client can wait for a response to a routing request.
**Late threshold.** The threshold value, in milliseconds, for classifying responses as late. Any response that exceeds this threshold is considered late even if it does not exceed the TimeoutThreshold.

**Timeout limit.** The maximum time, in seconds, for which the routing client waits for a response. If the routing client receives no responses from the ICM system within this limit, it terminates routing operation.

**Default call type.** The call type to be used for any route request that does not match a defined call type mapping. The drop-down list contains all configured call types.

ICM software uses the default call type for any routing request from the routing client that does not otherwise map to a call type. If you do not define a default call type for the routing client, ICM software uses a general default call type if you define one through the System Information command.

**Configuration parameters.** Leave blank for IPCC.

**Use DN/Label map.** Indicates whether only specific labels are valid for each dialed number associated with this routing client (when selected) or whether all labels associated with the routing client are valid for any dialed number (when not selected). Leave unchecked for IPCC.

**Client type.** Indicates the type of client. For the CCM peripheral, select IPCC/Enterprise Agent.

**Description.** Additional information about the routing client.

**Network routing client.** A name used to associate routing clients across instances.

**Network transfer preferred.** If checked, indicates that network transfer is preferred. When the target of a call is reachable by both a label defined for the requesting routing client and by another label defined for the network routing client that pre-routed the call, this option indicates which choice is preferred.

6. On the Default Route tab, select Cisco_Voice as the Media Routing Domain.

7. Click **Save**.

8. Once the record is saved, you can view the ID of a peripheral from the PG Explorer dialog. To view a peripheral record, start the PG Explorer from the Configuration Manager. The Logical controller ID is found on the Logical controller tab and the Peripheral ID displays on the Peripheral tab.

9. To add Peripherals for the IP-IVR and network VRU, click **Add Peripheral** and complete the information in the Peripheral and Routing Client tabs for each.

**How to Configure the VRU Peripheral**

To add a VRU Peripheral to your Generic PG, follow the same steps you used (above) to configure a CallManager Peripheral. When completing the tab fields, use the same values you used before, EXCEPT for the following:

1. On the Peripheral tab, use these values in place of those specified for the CallManager Peripheral:
   - **Name.** Enter value.
   - **Peripheral Name.** Enter value.
   - **Client type.** VRU
   - **Default desk setting.** None

2. On the Advanced tab, use these values in place of those specified for the CallManager Peripheral:
   - **Network VRU.** Select the type 2 network VRU you created earlier.
   - **Agent Auto Config.** Checked.
3. On the Agent Distribution tab, do not specify a distributor site name.
4. On the Routing Client tab, use these values in place of those specified for the CallManager peripheral:
   - **Name**: Enter value.
   - **Client type**: VRU

### How to Install the Generic PG

After the Generic PG has been configured, you then install the PG software on the PG machine. Before installing the Generic PG, record the Logical controller ID and Peripheral ID for the PG (from the PG Explorer).

**Note**

In the Setup screens, the Generic PG is referred to as the CallManager PG.

To install the Generic PG:

1. On the PG machine, from the ICM CD-ROM run setup.exe.
2. In the Instance Components section, select the ICM Instance to which you are adding the PG and click **Add** and choose **Peripheral Gateway** from the ICM Component Selection window.

**Note**

If the ICM instance which you want to add the PG has not been defined on this machine yet, use setup to create it before proceeding with the PG install. See the ICM installation documentation for more information on setting up instances.

3. Choose **Production Mode** and **Auto Start at System Startup** unless you are specifically told otherwise by your Cisco Support representative. This ensures that the Peripheral Gateway can restart itself automatically if necessary.
4. Specify whether the PG is part of a duplexed pair.
5. In the ID field, choose the PG’s device identifier as enabled in the CallRouter’s DMP configuration dialog box.
6. In the Client Type sections, add **CallManager/SoftACD** and **VRU** as the client types. Use the **Add** and **Remove** buttons to select or de-select PG types.
7. If the PG is duplexed, specify whether you are installing **Side A** or **Side B**. If the PG is simplex, select **Side A**.
8. Choose the local disk on which you want to install the PG software.
9. Choose the language.
10. Click **Next**. The Peripheral Gateway Component Properties window opens.
11. In the Peripheral Gateway Configuration section of the window, enter the Controller ID from the **Logical_Interface_Controller** record for the PG. The Controller ID is defined in ICM Configuration Manager when you configure the PG.
12. Click **Add** to add the PIM. You must add a PIM for each peripheral associated with the CallManager PG. All associated peripherals must be the CallManager type, as specified in the Setup Options dialog box.
13. Choose the PIM to add from the Available PIMs list. The list contains only PIM numbers that are not already defined for this PG. The CallManager/SoftACD Configuration dialog box appears in which you can enter the properties of the CallManager peripheral.

14. To put the PIM into service, check the Enabled option. This allows the PIM to communicate with the peripheral when the Peripheral Gateway is running.

15. Enter the peripheral name in the Peripheral name field. In most cases, you’ll want to use the enterprise name from the associated Peripheral record.

16. Enter the Peripheral ID from the Peripheral record.

17. Enter the number of digits in the agent extension.

18. In the Telephony Server Protocol section, choose CallManager as the type of application that you want to configure.

19. Complete the CallManager parameters section, as follows:
   a. Service: Enter the host name or the IP address of the primary CTI Manager in the CallManager cluster to which the PG connects. If using the host name, the name must be in the hosts file. For PG B, enter the host name or IP address of a backup CTI Manager in a CallManager cluster.
   b. User ID: Enter the User ID for the PG. This is the same User ID entered for the PG on the Cisco CallManager Administrator web page when you added the PG as a new user.
   c. User Password: Enter the User Password for the PG. This is the same User Password entered for the PG on the Cisco CallManager Administrator web page.
   d. Click OK.


21. If you prefer that the PG communicate with one side or the other of the Central Controller (for example, if the PG is collocated with one side), indicate the preferred side. Whether you specify a preferred side or not, if the PG cannot communicate with one side, it will automatically switch to the other.

22. Indicate whether the PG is local to or remote from each side of the Central Controller. If the PG is remote from either side, specify the maximum amount of bandwidth (in bits per second) the PG can use for communication with the CallRouter. Use this option to prevent the PG from overloading the wide-area network.

23. Indicate how often the PG should send heartbeats to the Central Controller. Specify the number of 100 millisecond intervals between heartbeats. For example, the default value of 4 means a heartbeat is sent every 400 milliseconds. The CallRouter considers the PG to be off-line if it misses five consecutive heartbeats. (By default, this occurs in two seconds.)

24. To configure the PG QoS settings, click Advanced. The PG QoS DMP Properties Advanced Options window displays.

25. Set the DSCP (DiffServ Codepoint) marking for each priority of the ICM traffic going to the Call Router. The defaults are acceptable if your network is Cisco AVVID compliant (Architecture for Voice, Video and Integrated Data). Otherwise, you need to consult your network administrator or Cisco representative for the proper values for these fields.

26. Uncheck the Bypass QoS packet scheduler box if you plan to use the Microsoft Packet Scheduler utility. This changes the appearance of the PG QoS DMP Properties Advanced Options window. The edit boxes for Medium Priority are grayed out and the Medium Priority always has the same settings as the High Priority. This is because Microsoft Packet Scheduler supports at most two classification levels (except best effort).
27. In addition to DSCP marking, the Class-of-Service (802.1p) marking is supported. The default values are set in compliance with Cisco AVVID recommendations. Consult your network administrator or Cisco representative for changes.

Note: Microsoft Packet Scheduler must be installed separately from the ICM setup if you uncheck the Bypass Packet Scheduler box. For more information about QoS for the ICM software, refer to the Pre-Installation Planning Guide for Cisco ICM Enterprise Edition.

28. Click OK to return to the Device Management Protocol Properties window.

29. Click Next. The Peripheral Gateway Network Configuration window displays. Enter the TCP/IP addresses or host name of the PG and, if it is duplexed, its pair. If the PG is simplex, enter localhost for the B side addresses. Also enter the visible network addresses for the CallRouter machines.

30. Click Next. The Check Setup Information window displays. Ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the Back button. When the settings are correct, click Next to begin copying files.

31. Click Finish to exit Setup and optionally start the Node Manager.

How to Install the Cisco JTAPI Client on the System or Generic PG

The Cisco JTAPI Client is a Java Telephony Application Programming Interface implementation that communicates with the Cisco CallManager.

After installing the System or Generic PG, you must install the Cisco JTAPI Client so that the PG can communicate via JTAPI with Cisco CallManager. You install the Cisco JTAPI Client from Cisco CallManager Administration.

To install the Cisco JTAPI Client:

1. Open a browser window on the PG machine.
2. Enter the URL for the CallManager Administration utility: http://<CallManager machine name>/ccmadmin.
3. Enter the user name and password that you created when installing and configuring Cisco CallManager.
5. Click the icon next to Cisco JTAPI. A File Download box opens.
6. Choose Run this program from its current location. Click OK.
7. On the Security Warning box, click Yes to install.
8. Choose Next or Continue through the remaining Setup screens. Accept the default installation path.
9. Click Finish.
10. Reboot the machine to ensure proper operation of JTAPI.
How to Configure and Install the Media Routing PG

If you are deploying Outbound Option or Multichannel applications, you must create Media Routing Peripheral Gateways in your IPCC Enterprise system.

To create a media routing peripheral gateway, use the ICM Configuration Manager’s Network VRU Explorer and the PG Explorer. You first configure the PG in the ICM Configuration Manager and then install the PG software on the PG machine(s).

For IPCC, you should configure peripherals for E-Mail Manager Option, Web Collaboration Option, and Outbound Option.

See Chapter 10, “Installing and Configuring Cisco Multichannel Components for IPCC Enterprise” for more information on how the MR-PG works.

How to Configure the MR-PG and Peripherals

You configure the MR-PG in the ICM Configuration Manager before installing the MR-PG software.

Tip

Record the Logical Controller ID and Physical Controller ID that are created when you save the MR-PG configuration. You need to enter these values when installing the MR-PG.

To configure the MR-PG:

You must configure a PG before you can install it. At the time you configure a new PG, you must add at least one peripheral to it or you will not be able to save the configuration.

1. In the ICM Configuration Manager, select Tools > Explorer Tools > PG Explorer.
2. Click Retrieve.
3. Click Add.
4. Complete the Logical Controller section as follows:
   - Logical Controller ID: Leave blank. This value will be auto-generated when the record is saved.
   - Physical Controller ID: Leave blank. This value will be auto-generated when the record is saved.
   - Name: Enter a unique enterprise name for the PG.
   - Client Type: Select MR PG.
   - Configuration Parameters: Leave blank.
   - Description: As desired, enter any other information about the PG.
   - Physical Controller Description: As desired, enter a description for the physical controller.

At this point, you are now ready to add the Outbound Option and/or multi-channel (E-Mail Manager, Web Collaboration) peripherals. Note that you will be unable to save the PG configuration you’ve entered thus far until you’ve added at least one peripheral.

How to Configure the MRPG Peripherals

To add peripherals to your MR PG, follow the same steps described earlier for configuring a CallManager peripheral. When completing the tab fields, use the same values you used before, EXCEPT for the following:

1. On the Peripheral tab, use these values in place of those specified for the CallManager peripheral:
How to Configure ICM for IPCC Enterprise

1. On the Client tab, do the following:
   - Client type. MR PG
   - Default desk setting. None
   - Post routing enabled. Checked

2. On the Advanced tab, use these values in place of those specified for the CallManager peripheral:
   - Network VRU. Select the type 2 network VRU you created earlier.
   - Agent Auto Config. Unchecked.

3. On the Agent Distribution tab, do not specify a distributor site name.

4. On the Routing Client tab, use these values in place of those specified for the CallManager peripheral:
   - Client type. MR PG
   - Network transfer preferred. Checked

5. On the Default Route tab, select Cisco Voice.

How to Install the MR-PG

When choosing where to install the MR PG, be aware you can only install two PGs per server. You must also consider the impact to overall performance. If you are installing the MR-PG in a laboratory environment, you can install the PG on the ICM sprawler machine.

For Web collaboration and E-Mail Manager options, you must configure one peripheral per application instance. For Outbound Option, you must configure one peripheral on the MR-PG per Dialer.

To install the Media Routing (MR) PG:

1. Run SETUP.EXE from the ICM CD-ROM on the machine that you want to make an MR-PG.
2. Select the IPCC instance.
3. Click Add in the Instance Components section.
4. Choose Peripheral Gateway from the ICM Component Selection window.
5. On the Peripheral Gateway Properties window, complete the following:
   - Choose Production Mode. Do not set the Auto Start feature until after installation is complete.
   - Specify whether the PG is part of a duplexed pair.
   - In the ID field, select the PG’s device identifier, as enabled in the CallRouter’s DMP configuration dialog box.
   - If the PG is duplexed, specify whether you are installing Side A or Side B. If the PG is simplex, select Side A.
   - Use the Client Type Selection section of the window to select MediaRouting and click Add.
   - Select the drive and language as appropriate and click Next.

The Peripheral Gateway Component Properties window displays.

6. Enter the Logical Controller ID generated when you configured the PG. Click the Add button and select PIM 1 from the list. The MediaRouting Configuration box displays.

7. Complete the following:
- To put the PIM into service, check the **Enabled** option. This allows the PIM to communicate with the peripheral when the Peripheral Gateway is running.

- Enter the peripheral name in the Peripheral name field. In most cases, you should use the enterprise name from the associated Peripheral record. When creating peripheral names, use short descriptive names and keep the length to a minimum. When creating peripheral names, use short descriptive names and keep the length to a minimum. Enter the Peripheral ID created when you configured the MR-PG.

- For Application Hostname (1): If you are configuring the Collaboration PIM, enter the IP address or hostname of the Media Blender machine. If you are configuring the E-Mail Manager PIM, enter the IP address or hostname of the E-Mail Manager application. If you are configuring the Outbound Option PIM, enter the IP address or hostname of the BA_IP Dialer.

- For Application Connection Port (1): For the Collaboration PIM, enter the connection port of the Media Blender machine. For the E-Mail Manager PIM, enter the connection port of the E-Mail Manager machine. For Outbound Option, enter the connection port that will be used by the BA_IP Dialer, usually 2000.

  **Note** When creating a PIM on the MR PG for Cisco E-Mail Manager, you must set the Application Connection Port to 1600 (default is 2000); set it to 2000 for the Cisco Collaboration Server. However, if you are also installing Outbound Option, it will use Port 2000 by default, so you need to be sure each application is using a different port. Be sure to make note of all port assignments because you will need them when you configure Collaboration Server, E-Mail Manager and Outbound Option.

Leave Application Hostname (2) blank.
Leave Application Connection Port (2) blank.

For Heartbeat Interval (seconds), specify how often the PG should check its connection to the application server. Use the default value.

For Reconnect Interval (seconds), specify how often the PG should try to re-establish a lost connection to the application server. Use the default value.

Click **OK**.

8. From the Peripheral Gateway Component Properties window, click **Next**. The Device Management Protocol Properties window displays.

Enter the appropriate settings and click **Next**. The Peripheral Gateway Network Interfaces window displays.

Enter the appropriate settings and click **Next**. The Check Setup Information window displays.

9. Verify the setup information and click **Next**. ICM software installs the PG.

10. When the Setup Complete window displays, click **Finish** to exit from the setup program.

**How to Configure Trunk Groups**

For IPCC, the **Network Trunk Group** is the placeholder in the ICM database for the Trunk Group; it performs no other function. For deployments that:

- Use the System PG, you must create one Network Trunk Group for each IPCC System PG peripheral.
• Do not use the System PG, you must create two Network Trunk Groups: one for CallManager and one for IP IVR or CVP. If you are deploying CVP, create one Network Trunk Group per Application Server.

A trunk is a telephone line connected to a call center and used for incoming or outgoing calls. An ICM Trunk Group is a collection of trunks associated with a single peripheral and usually used for a common purpose. For IPCC Enterprise, the Trunk Groups for VRU peripherals are used primarily as a placeholder in the ICM database.

Create a Trunk Group for each CallManager peripheral and a trunk group for each IP IVR application. For IP IVR, the Trunk Group peripheral number in ICM must match the CTI Port Group ID on IP IVR. If you are deploying CVP, you must create two Trunk Groups for each CVP Application Server that match the Group Numbers configured in CVP Application Administration.

This section describes how to configure individual Network Trunk groups and Trunk Groups. You can also configure them in bulk.

To configure a Network Trunk Group (and the Trunk Group under it) in ICM software:

1. From the Configuration Manager, choose Configure ICM > Peripherals > Trunk Group > Network Trunk Group Explorer. The ICM Network Trunk Group Explorer dialog box opens.
2. Click Retrieve.
3. Click Add Network Trunk Group. The Network trunk group tab opens.
4. Add a unique name for the network trunk group and an appropriate description.
5. Click Add Trunk Group to add a trunk group.
6. Complete these fields:
   - Peripheral. Select the peripheral to which the trunk group is associated.
   - Peripheral Number. Enter the number of the trunk group as understood by the peripheral. This number must be unique among all trunk groups associated with the peripheral.
     - For IP IVR, this number must: A) match a CTI Port Group ID configured on the IP IVR, B) be an odd number, and C) be unique for all IP IVR handled by a System PG. For example, if a System PG handles four IP IVRs and each IP IVR peripheral has one CTI Port Group, then the CTI Port Group ID for the first IP IVR should be 1, the port group ID for the second IP IVR should be 3, and so on.
     - For CVP, this number must match an Application Server Group Number configured on the Application Server.
   - Peripheral Name. Enter the name of the trunk group as understood by the peripheral. This name must be unique among all trunk groups associated with the peripheral.
   - Name. Enter the enterprise name of the trunk group. ICM software forms a default for this name using the entries from the Peripheral and Peripheral Name fields.
   - Extension. Leave this field blank.
   - Trunk Count. Select Use Trunk Data.
   - Config. Param. Leave this field blank.
   - Description. Enter an optional description.
7. To add Trunks to the Trunk Group, click Add Trunk.
8. Add trunks as desired.
9. Save and then click Close.
10. Repeat to create all necessary trunk groups.

**How to Configure the Network VRU Bank**

For deployments that use the System PG, after the Network VRU, the network trunk group, and all the trunk groups have been configured, the next step is to configure the Network VRU Bank. The Network VRU Bank allows load balancing across multiple VRUs to occur and eliminates the need for complex translation-route configuration.

To configure the Network VRU Bank:

1. From the Configuration Manager, choose **Explorer Tools > Network VRU Explorer**. The Network VRU Explorer dialog box opens.
2. Click **Retrieve**.
3. Select your network VRU.
4. Select the Network VRU Bank tab and click **Add**.
5. The Select Trunk Group dialog opens, displaying the all trunk groups configured on all IPCC System PG peripherals. Select the trunk group associated with the translation routing group on your IP IVR. Make the appropriate trunk group selection for each IP IVR in your deployment.
6. Click **OK**.
7. Click **Add Label** to add a label for the Network VRU Bank. The label must be the CTI Route Point trigger for the Translation-Routing application on the IP IVR.

**How to Configure Services**

A service refers to a type of processing that a caller requires. For example, separate services might be defined for Sales, Support, or Accounts Payable. Services are often associated with a peripheral, and are sometimes referred to as peripheral services. An agent will be assigned one or more skills that in turn will be associated with services. Routing to an ICM service effectively targets an agent assigned to an ICM skill group associated with the ICM service.

Services on ICM correspond to CTI Route Points on Cisco CallManager.

For CVP, you must configure 2 Services with Peripheral Numbers of 1 and 2.

**Note**

For the two CVP Services, you do not need to configure Service Members, Routes, Peripheral Targets, or Labels.

This section describes how to configure individual Services. You can also create these records in bulk using the Bulk Configuration Tool.

To configure a service:

1. From the ICM Configuration Manager menu, choose **Tools > Service Explorer**. The ICM Service Explorer dialog box opens.
2. Select the peripheral for which you want to create a service and Click **Retrieve**.
3. Click **Add Service**. The Service Configuration window opens.
4. On the Service tab, enter the following:
Media Routing Domain.

**Peripheral Number.** Choose number as known at the peripheral. This field must be unique for all services for the peripheral, but not necessarily across all peripherals. If you are deploying CVP, enter 1 for the first service and 2 for the second service.

**Peripheral Name.** Enter a name that describes the Service.

**Enterprise Name.** Enter an enterprise name for the service. This name must be unique among all the services in the enterprise. If you do not enter a value, this name will autogenerated.

**Config Param.** Not used for IPCC.

**Description.** Enter any additional information about the service.

**Service Level Type.** Indicates how ICM software calculates the service level for the service. You can choose to omit abandoned calls from the calculation, treat them as having exceeded the threshold (negative impact on service level), or treat them as answered calls (positive impact on service level). You can also choose to use the default specified for the peripheral.

**Service Level Threshold.** Enter the time in seconds, for the ICM service level. ICM software tracks the percentage of calls answered within this threshold. If this field is negative, the value of the default for the peripheral is used.

5. On the Advanced tab, enter the following

**Peripheral Service Level.** Indicates the type of service level calculation that the peripheral performs for this service. This setting has no effect since the PG does not report a peripheral service level.

**Extension.** On the Advanced tab, If you are deploying Outbound Option, enter the extension to associate with this service. This corresponds to a CTI Route Point defined in CallManager and is associated with the PG User.

6. On the Service Members tab, select skill groups to associate with this service.

7. Click the **Apply** button.

8. Repeat this procedure to add any other services.

### How to Configure Skill Groups

A skill group is a collection of agents that share a common set of skills. Skill groups are associated with a peripheral and are referred to as Peripheral Skill Groups. Skill groups are generally members of Services. IPCC agents are assigned one or more skills by associating the agent with the desired skill. The set of skills the agent is associated with will be agent default skills. When an agent logs in, the agent will be assigned the default skills. Default skills are configured in the ICM database.

After you have created Services and skill groups, you associate one or more skill groups with a service by making them members of that service.

This section describes how to configure individual skill groups. You can also create these records in bulk using the Bulk Configuration Tool.

**Note**

An IPCC agent must be assigned to at least one skill group in order to log in.

This section describes:

- About Default Skill Groups, page 6-28
About Default Skill Groups

The default skill group acts as a bucket to capture information about calls not routed by ICM routing scripts.

A default skill group captures call statistics for calls that are not routed by an ICM routing script. A call placed directly to an agent's extension is an example of such a scenario. Using a default skill group helps to:

- Ensure the agent/skill group reports balance with the service and call type reports, since service and call type reports include only ICM-routed calls.
- Isolate/identify non-ICM-routed calls within the agent and skill group report.

You do not have to create a default skill group—it is automatically created when you establish Peripheral Gateways for your system. The default skill group has a peripheral number of 0.

If you deploy Multichannel options in your IPCC Enterprise system, default skill groups are created for each Media Routing Domain that you configure. See Chapter 10, “Installing and Configuring Cisco Multichannel Components for IPCC Enterprise” for more information.

About the “ICM picks the agent” Skill Group Attribute

“ICM picks the agent” (IPTA) means that the ICM central controller is responsible for selecting the actual agent who will handle a request, not just the service or skill group. For each skill group that you configure using the ICM Configuration Manager, you select whether ICM picks the agent when routing calls to that skill group.

In legacy ICM Enterprise deployments, the ICM central controller determines which Automated Call Distributor (ACD) has the appropriate service or skill group to handle a request and the ACD selects the actual agent to handle the call. The ICM central controller pre-routes calls by targeting an ACD and the ACD post-routes calls by selecting the agent.

In an IPCC Enterprise environment, the ICM central controller handles the post-routing of requests to agents. Choose the “ICM picks the agent” option for all skill groups that you configure for IPCC Enterprise.

For the Web Collaboration Option and E-Mail Manager Options, you create skill groups and determine whether ICM picks the agent using the administration tools for these options. If you want to utilize the Universal Queue feature, these skill groups must enable the ICM central controller to pick the agent. See Chapter 10, “Installing and Configuring Cisco Multichannel Components for IPCC Enterprise” for more information.

The IPCC Enterprise Generic Event Link feature introduces a layer of complexity to IPTA. In IPCC Enterprise Generic Event Link configurations, the IPCC Enterprise’s central controller pre-routes voice calls to an IPCC Enterprise system, and the IPCC Enterprise’s central controller selects the agent to handle the calls.
In an IPCC Enterprise Generic Event Link configuration, the ICM Enterprise’s central controller can route only voice calls to the IPCC Enterprise system; it cannot route non-voice requests, such as text chat and E-mail, or Outbound Option requests. Non-voice requests and Outbound Option requests are routed internally by the IPCC Enterprise system.

**How to Configure Skill Groups**

You configure skill groups in ICM software using the ICM Configuration Manager Skill Group Explorer tool. In addition to configuring skill groups, you can also use this tool to configure routes, peripheral targets (DNIS) and labels.

**Note** Cisco recommends that you configure only base skill groups for IPCC. Sub-skill groups, while supported, are not recommended.

You configure skill groups for single-session chat, multi-session chat, Blended Collaboration, and E-mail in the Web collaboration and E-Mail Manager options, not in the ICM Configuration Manager.

To configure a skill group:

1. From the ICM Configuration Manager, choose **Configure ICM > Peripherals > Skill Group > Skill Group Explorer**. The ICM Skill Group Explorer dialog box opens.

2. In the Select filter data section, select the peripheral from the drop-down list.

3. Click **Retrieve** and then click **Add Skill group** to add a new skill group for the selected peripheral.

4. Click the Skill Group tab and enter values for the following:
   - **Media Routing Domain.** Use Cisco_Voice for ICM agents that will not use other media. Do not create skill groups for the Multichannel applications using ICM software. See Chapter 10, “Installing and Configuring Cisco Multichannel Components for IPCC Enterprise” for more information.
   - **Peripheral Number.** Enter the skill group number as known by the peripheral. This value must be unique among all skill groups for the peripheral, but does not need to be unique across peripherals.
   - **Peripheral Name.** Enter the local name for the skill group. This value must be unique among all skill groups for the peripheral, but does not need to be unique across peripherals.
   - **Name.** The ICM Configuration Manager generates the value for this field. This is a unique name for the skill group made up of a default value from the peripheral’s enterprise name and the skill group’s peripheral name.
   - **Available Holdoff Delay.** For the IPCC peripheral type, set this field to 0.
   - **Priority.** This is a read-only field and defaults to 0.
   - **Extension.** Leave blank for the IPCC peripheral type.
   - **ConfigParam.** Leave blank for the IPCC peripheral type.
   - **Description.** Enter any additional information about the skill group.
   - **ICM picks the agent.** Select this check box.

5. Click **Save** and then click **Close**.

6. Repeat this procedure to add any additional skill groups.
How to Configure Service Members

To make a skill group a member of a Service, you establish mappings of skill groups to Services. Each skill group can be mapped to zero, one, or more Services. Each Service can have zero, one, or more skill group members. By mapping skill groups to Services, you create an organizational structure that allows you the maximum flexibility in routing calls to the correct agents.

Note

If you are using the Multichannel options (Web collaboration and E-Mail Manager), these applications automatically create a Service and a Route for each skill group they create in ICM software, and you do not have to associate a Service for these skill groups.

To associate a skill group with a Service:

1. From the ICM Configuration Manager, choose Configure ICM > Peripherals > Service > Service Explorer. The ICM Service Explorer dialog box opens.
2. Click Retrieve.
3. Click the Service that directs the skill group and then click the Service Members tab.
4. Click the Service Members tab and click Add to associate a skill group with the service.
5. Click OK.
6. Repeat this procedure for each skill group that you want to associate.
7. Click Save and then click Close.

How to Configure Persons

All IPCC agents must have a Person record. When you create an Agent record (see How to Configure Agents, page 6-31), you have the option to associate the record with an existing Person record. If you do not associate the Agent record with an existing Person record, a new Person record is automatically created when you create the agent.

Note

If your agent will use Multichannel applications, such as E-Mail and Web collaboration, you should create your agent in one of these Multichannel applications. Agent and Person records are created automatically in both the Multichannel application database and the ICM database. Also, you do not need to create a Person or Agent record using ICM Configuration Manager.

This section describes how to configure individual Persons. You can also create these records in bulk using the Bulk Configuration Tool.

To configure a Person record before configuring an agent:

1. From the ICM Configuration Manager, choose Peripherals > Person > Person List. The Person List dialog box opens.
2. Click Retrieve and then click Add.
3. Enter information in the following fields of the Attributes tab:
   - First Name. Enter the person’s first name.
   - Last Name. Enter the person’s last name.
   - Login Name. Enter the person’s login name.
**How to Configure Agents**

The agent is the person who responds to requests from the customer. Agents can work on tasks involving several media types, such as e-mail, chat, and voice. Agents must be associated with a peripheral and be a member of one or more skill groups. You can also group agents into agent teams.

To create an Agent record, you must associate a Person with the agent. For an existing Agent record, you can select a different Person (from the current one selected) to be associated with that agent record. If you select a person for a temporary agent, you make that agent permanent. You cannot demote an agent to be a temporary one.

An ICM agent’s personal information is stored in the database’s Person table.

This section describes how to configure individual agents. You can also create these records in bulk using the Bulk Configuration Tool.

This section describes:

- How to Configure Agents, page 6-31
- How to Configure Agent Supervisors, page 6-32
- How to Assign Agents to Skill Groups, page 6-32
- How to Configure Agent Teams, page 6-33
- About Supervisory Features, page 6-34

**How to Configure Agents**

You configure agents using the Agent Explorer.

To configure an agent:

1. Select **Tools > Explorer Tools > Agent Explorer**. The Agent Explorer window displays.
2. Select the peripheral you want associated with the agent from the drop-down list and click **Retrieve**.
3. Click **Add Agent** to display the Agent configuration tab.
4. In the Agent tab, enter the following:
   - **Last Name**: Enter the agent’s last name.
   - **First Name**: Enter the agent’s first name.
   - **Login Name**: Enter the name the agent uses to login. This name must be unique in the enterprise.
   - **Password**: Enter the agent’s password. This password is validated during the agent login process.
   - **Login Enabled**: Check this box if you want the enable the agent to login.
   - **Select Person**: Click this button to select a person to associate with the agent record. You can select a person for a new agent, an existing agent, or a temporary agent.
   - **Enterprise Name**: Enter an enterprise name for the agent that is unique within the enterprise. The default is a combination of the peripheral name with the agent’s first and last name.
Peripheral Name. Enter a name for the agent as known to the peripheral.

Peripheral Number. Enter the agent’s login ID. This number identifies the agent to the peripheral. This number needs to be unique among all agents for the peripheral, but does not need to be unique across all peripherals.

Agent IDs can be up to nine digits long. The first digit in the ID must be 1 through 9. It cannot be 0. Also, this number cannot be the same as the extensions on the Cisco CallManager cluster for this agent. Finally, the ID cannot exceed the extension length specified in the CallManager PG setup.

5. Click the Advanced Tab and enter:

Desk Setting. Use the drop-down list to select the desktop settings to be associated with the agent. If you do not make a selection, ICM software applies the default desk settings defined for the peripheral.

ConfigParam. Use this field to enter any specific configuration parameters that may be required. Make entries in this field only if instructed to do so by your Cisco support representative.

Description. Enter any other information you want about the agent.

Agent State Trace. Select to enable the agent’s state trace control. When enabled, ICM software will record every state transition made by the agent.

6. Click Save.

7. Repeat this process to configure additional agents.

How to Configure Agent Supervisors

When you create an agent, you can assign that agent to be an agent supervisor.

To assign an agent to be a supervisor:

1. On the open Agent Explorer for the agent that you want to make a supervisor, click the Supervisor tab.

2. Enter the following:

   Supervisor Agent. Check this box to indicate that the selected agent is a supervisor.

   Domain name. Enter the Windows NT or Windows 2000 domain name. This is the unique host name on the Internet to which the user group belongs.

   Supervisor login as user. Enter the NT user ID of the selected agent. This entry cannot be the NT Administrator account.

   Description. Enter an optional description for the supervisor.

How to Assign Agents to Skill Groups

Agents must be assigned to at least one skill group in order to log in. You can assign agents to the most appropriate skill groups according to their talents and skills to ensure that the most appropriate agent for a request responds to the customer.
How to Configure ICM for IPCC Enterprise

Note You can assign agents to Web collaboration and E-Mail Manager skill groups only using the Web collaboration and E-Mail Manager applications, not using the ICM Configuration Manager.

To assign an agent to one or more skill groups:
1. From the Agent Explorer dialog box, choose the Skill Group Membership tab.
2. From the Skill group name list, select the skill groups to which you want this agent assigned.
3. Click Add. The Add Skill Group Membership box opens, showing the skill groups to which the agent has been assigned.
4. Click OK.
5. Click Save and then click Close on the Agent Explorer dialog box.
6. Repeat this procedure to assign additional agents to skill groups.

Note You can remove agents from the Skill Group tab if necessary by selecting the agent and clicking Remove, then Save.

How to Configure Agent Teams

ICM software allows you to group individual agents into agent teams that can be managed by supervisors. Agent teams are assigned to specific peripherals, so all agents of a given team must be assigned to the same peripheral.

Agents are assigned to agent teams individually. When configuring agent teams, you should be aware of the following rules:

• An agent can be a member of only one agent team.
• An agent team can have only one Primary Supervisor.
• A supervisor can be a supervisor of any number of agent teams.
• A supervisor for an agent team can also be a member of that agent team.
• All agents belonging to an agent team and all supervisors for that agent team must be on the same peripheral.
• A supervisor cannot use the NT administrator account when logging in as supervisor.

To configure an agent team and assign agents to the team:
1. From the Configuration Manager, select Configure ICM > Peripherals > Agent Team > Agent Team List.
2. Click Retrieve and then Add to add a new agent team.
3. Click the Attributes tab and enter values for the following:
   Name. Enter an enterprise name for the agent team that is unique within the enterprise.
   Peripheral: Enter the name of the agent team peripheral. You can select the name from the drop-down list.
   Supervisor Script Dialed Number: Select a dialed number for the agent team from the drop-down list. If you have not created a supervisor script, select the default, “none”. When you create the script, return to this screen and enter the dialed number for the script.
**Description:** Enter additional information about the agent team.

4. Click the **Members** tab and click **Add**.

5. Choose the agents that you want to assign to the team and click **OK**.

6. Click the **Supervisor** tab and choose the supervisor from the Primary Supervisor pull-down list.

7. To add a secondary supervisor, click the **Add** button and select a secondary supervisor from the list. Click **OK**.

8. Click **Save** and then click **Close**.

---

**About Supervisory Features**

Supervisors of agent teams can take advantage of supervisory features available with their Agent Desktop software. The following table describes these features.

Refer to the *IPCC Administration Guide for Cisco IPCC Enterprise Edition* for more information on setting up Supervisory features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor and emergency assist</td>
<td>An agent can activate supervisor assist or emergency assist buttons on the desktop when he/she needs special assistance from the primary or secondary supervisor assigned to his/her team. There are two types of supervisory assist calls: existing calls (consultative) and no call.</td>
</tr>
<tr>
<td></td>
<td><strong>Existing call:</strong> Consult must be selected as an option on the agent desktop settings for supervisor or emergency assist. If the agent is on a call when s/he activates either the supervisor or emergency assist feature on her/his desktop, the CTI software activates the conference key on behalf of the agent's phone and calls the supervisor via the Supervisor or Emergency Assist script. (This example assumes the emergency or supervisor assist script has an Agent-to-Agent node to find a supervisor.) The supervisor answers the call and consult privately with the agent. During the consultation, the supervisor can decide to barge into the call.</td>
</tr>
<tr>
<td></td>
<td><strong>No call:</strong> If the agent is not on a call when he or she activates either the supervisor or emergency assist feature on the agent's desktop: the CTI software activates the make call functionality on behalf of the agent’s phone and calls the supervisor via the Supervisor or Emergency Assist script.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Blind Conference is not supported for Emergency and Supervisor Assist</td>
</tr>
<tr>
<td>Barge-in</td>
<td>When the supervisor activates the Barge-in feature from his or her desktop, the agent’s desktop completes a conference to the supervisor, so that the supervisor can join into the conversation with the call.</td>
</tr>
<tr>
<td>Intercept</td>
<td>If the supervisor decides to intercept (take over) the call, the supervisor activates the Intercept button on his or her desktop. This causes the agent to be dropped out of the conference, thereby allowing the supervisor to take over the call.</td>
</tr>
</tbody>
</table>
How to Configure Dialed Numbers

The dialed number is the number that the caller dials to initiate the call and identifies the ICM routing script that should be run. Dialed numbers also need to be set up for ring on no answer, dialed number plan entries, and for Supervisor/emergency calls.

The ICM software generates a unique value for the Label Name list after you configuring a dialed number.

This section describes how to configure individual dialed numbers. You can also create these records in bulk using the Bulk Configuration Tool.

To configure a dialed number:

1. From the ICM Configuration Manager, choose Tools > List Tools > Dialed Number List. The ICM Dialed Number List dialog box opens.
2. Click Retrieve and then click the Add. The Attributes tab displays.
3. Enter values for the following fields in the Attributes tab:
   - **Routing client.** Choose the enterprise name of the routing client associated with this dialed number. Once you select a routing client and save to the database, this field becomes read only.
   - **Media Routing Domain**
   - **Dialed number string.** Enter the string value that the routing client passes to the ICM for this dialed number (for example: 8005551212).
   - **Name.** Enter the enterprise name for the dialed number. This name must be unique among all dialed numbers in the system. If you do not enter a value, this will be autogenerated.
   - **Customer.** Use the drop-down list to select the customer (ICM instance) associated with the dialed number.
   - **Default label.** Choose the name of the default label for this dialed number. The label must have been previously defined for it to be in the selection list. Use the ICM Configuration Manager’s Label List tool to define labels.
     - If ICM software fails to determine a target for the call within the routing client’s time-out threshold, then the default label for the dialed number is used.
   - **Description.** Enter a description for the dialed number.
   - **Reserved by IVR.** For IVR dialed numbers, Reserved by IVR must be checked. This prevents the Call Manager PIM from trying to exert control on the calls arriving on these Route Points.
4. On the DN Mapping tab, as desired, click Add to specify a Calltype and other dialing information to associate with this dialed number.
5. Click Save to enter the dialed number information.
6. Repeat this procedure to add any additional dialed numbers.

How to Configure Routes

The route is a value returned by a routing script that maps to a target or a peripheral. Those targets include services, skill groups, agents, translation routes, queue points, or CTI route points. ICM software converts a route to a label (for ACDs) or a device target (for IPCC) to direct to the destination of a request.

When you create a route, you associate the route with a service.
This section describes how to configure individual routes. You can also create these records in bulk using the Bulk Configuration Tool.

To configure a route for a skill group:

1. From the ICM Configuration manager, choose **Explorer Tools > Skill Group Explorer.** The ICM Skill Group Explorer dialog box opens.
2. Click **Retrieve.**
3. Choose the skill group for which you are creating the route.
4. Click **Add Route.**
5. The Route tab opens.
6. In the Route tab, enter values for the following fields:
   - **Name.** Enter a unique name for the route. You might derive the name for the route from the skill target and service associated with it. Use this convention for the name: `[Peripheral]_[SVC, SG, AG]_[DNIS]`. The lab value below follows this convention.
   - **Description.** Enter an optional description of the route.
   - **Service Name:** Lab Value: None
7. Click **Save.**

**Warning**
When you break the association between a route and a peripheral, ICM software removes the Route ID value from all peripheral targets that reference that route.

### How to Configure Device Targets

**Note**
This step is not required for deployments that use the System PG.

IPCC systems require that a device target be configured for each IP telephone that may be used by an agent. A device target is a telephony device that can be uniquely addressed by a telephone number. A device target is not associated with any one peripheral. Each device target must have one or more associated labels, although only one label may exist per routing client. ICM software uses the device target to locate the label that will route a call to an IPCC agent.

An agent is dynamically associated to a device target at the time the agent logs into a peripheral. The agent log-in request will specify the device target, or targets, to be associated with the agent. The association between the agent and the device target lasts until the agent logs out of the peripheral.

After you have configured device targets, you can verify that you have configured agents properly in the ICM by placing an Agent to Agent call. This test verifies your installation and configuration of the JTAPI client, CTI OS and agents in the ICM software. To verify agent configuration, you need to log in as an agent and then make a call to another agent. Note that calling another agent requires that you use the agent id and not the phone number of the instrument.

This section describes how to configure individual device targets. You can also create these records in bulk using the Bulk Configuration Tool.
To configure a device target:

1. From the ICM Configuration Manager, choose Configure ICM > Targets > Device Target > Device Target Explorer. The Device Target Explorer window opens.
2. Click Retrieve and then click Add Device Target. The Device Target tab opens.
3. Enter values for the following fields:
   - **Name**: Enter an enterprise name for the target. This name must be unique among all device targets in the enterprise.
   - **Global Address**: Enter the global address for the device. Must be set to a value that is unique from all other device targets in the enterprise. It is suggested that you use the same value that you entered in the Enterprise Name field.
   - **Config Parameters**: Use this field to enter any specific configuration parameters that may be required:
     - `/devtype (CiscoPhone)`
     - `/dn (full phone number) /ext (extension)`
     The ICM software gives this string to the Cisco CallManager to initialize the device. Using the extension (ext) may be optional, depending on your environment. In most cases, using the dialed number (dn) is sufficient. The dn must start with a number 1 through 9 (0 is not allowed), and the extension length must match the length that you indicated in the CallManager PG setup.
   - **Description**: Enter a description of the device. This is an optional field used to provide additional information about the device.
4. When you are done entering the Device Target information, click the **Save** button.

### How to Configure Labels

**Note** This step is not required for deployments that use the System PG.

Labels are required for device targets and VRU services for IPCC. The ICM Script Editor requires that you create scripts targeting a skill group or service. The skill group or service identifies a set of routes to a peripheral, which in turn identifies a set of device targets.

ICM software returns labels to routing clients that have requested a route. The routing client uses the label to deliver the task. With IPCC, the routing label is associated with the Device Target. ICM software also requires a label when sending a call to a CTI Route Point or VRU.

Special labels might instruct the routing client to take another action such as play a busy signal or an unanswered ring to the caller.

ICM software can select a logged-on and available agent using one of the many selection criteria available in the ICM Scripting Language. Given the agent, ICM software chooses an associated Device Target based on the type of resource requested.

This section describes how to configure individual labels. You can also create these records in bulk using the Bulk Configuration Tool.

To configure a label:
1. In the Device Targets Explorer window, select the target (service) for which you are creating the label and click Add Label.
2. In the Label tab, enter values for the following fields:
   - **Routing Client.** Select the enterprise name of the routing client that can receive the label. You must configure a label for each type of IPCC routing client, including the interexchange carriers, NICs, network VRUs and post-routing PGs.
   - **Label.** Enter the literal string of characters to be returned to the routing client.
   - **Label Type.** Enter the label type. The label type for IPCC is Normal.
   - **Customer.** Choose the customer (ICM Instance) from the drop-down list.
   - **Description.** Enter optional information about the label.
3. Click Save to save the network target settings.
4. Repeat this procedure to add additional labels.
   ICM software generates a unique value for the Label Name list after you save the attributes.

### How to Configure Call Types

A call type is a category of ICM routable task. Each call type has a schedule that determines which routing script or scripts are active for that call type at any time. There are two classes of call types:

- **Voice (phone calls).** Voice call types are categorized by the dialed number (DN), caller-entered digits (CED), and calling line ID (CLID). The CED and CLID can be optional, depending on the call.
- **Non-voice (e-mail and text chat).** Non-voice call types are categorized by the Script Type Selector, Application String 1, and Application String 2. Application String 1 and Application String 2 can be optional, depending on the application.

This section describes how to configure individual call types. You can also create these records in bulk using the Bulk Configuration Tool.

To configure call types:

1. From the ICM Configuration Manager, select **Tools > List Tools > Call Type List.** The Call Type List dialog box opens. Click **Retrieve** and then click **Add.** The Attributes tab displays.
2. Enter values for the following fields in the Attributes tab:
   - **Name.** Enter an enterprise name for the call type. This name must be unique among call types in the system.
   - **Customer.** Choose the customer (ICM Instance) from the drop-down list.
   - **Service level threshold.** Enter the number of seconds for the service level threshold. The number of seconds you set as the maximum time a caller should wait before being connected with an agent for a specific service. When you set up a peripheral, you specify a default service level threshold for all services associated with that peripheral. If you enter a negative number, the service level threshold from the Peripheral table is used.
   - **Service level type.** Choose the service level type from the drop-down list to indicate how you want ICM software to handle abandoned calls when calculating the service level. The default is the level specified for the associated peripheral.
Description. Enter an optional description of the call type.

3. Click Save to enter the call type information.

4. Repeat this procedure to add additional call types.

5. Create an additional call type named outbound_calltype

Note To facilitate IPCC reporting, it is good practice to create separate call types for IVR applications and queueing applications.

How to Configure Translation Routes

Use the Translation Route wizard to configure the translation routes for the CallManager and VRU peripherals. This wizard automates the correct associations with peripheral targets, labels, and routes.

Note Run the Translation Route Wizard only if you have included the Generic PG or CVP in your IPCC System.

To create translation routes with the wizard:

1. In the ICM Configuration Manager, select Tools > Wizards > Translation Route Wizard. The Translation Route Wizard introductory dialog box opens.

2. Click Next. The Acquire Lock and Select Configuration Task dialog box opens.

3. Choose Create New.

4. Click Next. The Define Translation Route dialog box opens. The graphic on the left of the dialog box shows the entities you will be defining while using the Translation Route Wizard.

5. Enter a long and short name for the translation route and, optionally, a description (the short name is used in forming target names).

6. Click Next. The Select Configuration dialog box opens.

7. Choose the single peripheral, single routing client configuration from the drop-down list. The graphic changes to show the configuration you select.

8. Click Next. The Select Peripheral Gateway, Peripherals, and Services dialog box opens.

9. Enter values for the following:
   - Peripheral Gateway. Choose the gateway target for the translation route.
   - Peripheral. Choose the single peripheral or the peripheral to route calls to.
   - Service/Service Array. If the translation route is associated with a single peripheral, choose the service associated with the translation route. If the translation route is associated with multiple VRUs, then select a service array.

10. Click Next. The Select Routing Clients and Dialed Numbers opens. Use this dialog box to specify the CallManager peripheral (or VRU peripheral) as the routing client from which translation routed calls originate. For IPCC the dialed number string is not applicable.

11. Click Next. The Select Network Trunk Groups for Routing Clients dialog box opens. Choose at least one network trunk group to be used in peripheral targets associated with the translation route.

12. Choose a routing client, select a network trunk group value for it, and click Add. The Network Trunk Group appears in the list at the bottom of the dialog box.
13. Click **Next**. The Configure DNIS dialog box opens. Use this dialog box to specify the DNIS values that map to route points on the VRU. Do one of the following:
   - To enter a specific DNIS value, click **Add DNIS** and enter the value.
   - To add a range of DNIS values, typically required by a translation route, click **Add DNIS Range**. A dialog box prompts you to enter a starting and ending DNIS value. The Translation Route Wizard automatically generates the DNIS values in the range.

14. Click **Next**. The Configure Label dialog box appears. Use this dialog box to define a label that maps to the DNIS/CTI route points. A label consists of a prefix and a suffix. Each DNIS value requires a unique label. Do one of the following:
   - Enter prefixes and suffixes individually.
   - Use the buttons in this dialog box to set a range of values or to base the prefix or suffix values on the DNIS values.

15. Click **Next**. The Wizard Complete dialog box opens.

16. Click **Create Translation Route** to create the translation route and its associated entities. First, the Translation Route Wizard displays a success message and then the dialog box appears as follows.

17. Do one of the following:
   - To see details about the translation route you just created, click **Run Report**.
   - To return to the beginning of the Translation Route Wizard and perform a new task, select **Start New Task** and click **Finish**.
   - To exit the Translation Route Wizard, click **Finish**.

### How to Configure Network VRU Scripts

VRU Scripts differ from ICM routing scripts. A configured VRU Script runs only when ICM instructs it to do so from an ICM routing script. A VRU Script on ICM is the configured record for the VRU script that resides on the IP-IVR. A VRU Script executes to collect digits, play hold music, or perform many other common IVR functions.

After you configure a Network VRU Script, you can access the VRU in ICM scripts, troubleshoot scripts, and perform VRU error checking.

This section describes how to configure individual Network VRU Scripts. You can also create these records in bulk using the Bulk Configuration Tool.

This section describes:

- How to Configure a Network VRU Script, page 6-40
- How to Access VRUs in ICM Scripts, page 6-41
- About Troubleshooting Scripts, page 6-41
- About VRU Error Checking, page 6-42

### How to Configure a Network VRU Script

To configure a VRU Script:

1. From the ICM Configuration Manager, select **Tools > List Tools > Network VRU Script List**. The Network VRU Script List dialog box opens.

2. Click **Retrieve**.
3. Click Add.

4. On the Attributes tab, enter the configuration information for the BasicQ script as follows:
   - **Network VRU.** Specify the network VRU with which this script should be associated.
   - **VRU Script Name.** Enter script name (i.e. BasicQ)
   - **Name.** Enter the script file name (i.e. BasicQ.aef)
   - **Timeout [seconds].** Enter 180.
   - **Configuration param.** Leave blank.
   - **Customer.** Choose the same ICM customer you chose for Call Type from the drop-down list.

5. Select the **Interruptible** check box.

6. Click **Save** and then click **Close**.

---

**Note**

Before you can use a VRU script, you must upload it to the Repository in IP-IVR. See **How to Configure and Upload VRU Scripts, page 5-9**.

---

**How to Access VRUs in ICM Scripts**

After you have configured a Network IVR and IVR scripts, you can use the Script Editor to write a routing script to send a call to the VRU and invoke a specific VRU script.

For deployments that include CVP and/or the Generic PG for VRU and CallManager, you use the Translation Route to VRU node to send calls to the Network IVR and invoke IVR scripts. Translation Route to VRU node should not be used for deployments that use the System PG. Instead, use any one of Queue to Skill Group or Send to VRU nodes.

**About Troubleshooting Scripts**

In the event of a timeout on a VRU script, it is possible that the CallRouter does not notify the VRU PIM that a timeout has occurred. Since the VRU PIM is not informed of the problem, it does not notify the VRU to cancel the script. At this point the options for script flow include the following:

- The failure path in the CallRouter script sends the call to a label, the VRU PIM gets a Connect and, if the IVR supports it, generates a Cancel message. This is the most common result.
- Before the CallRouter picks a label, the VRU script completes and the VRU sends a Script Result message to the CallRouter. The CallRouter then sends a Dialogue Failure Event because is not expecting a Script Result. This is the next most common result.
- The failure path in the CallRouter script tries to run another VRU script. This is not a common result.

Currently the best resolution to this problem is to use longer time-outs or create shorter VRU scripts, and be aware that the failure exit from the Run VRU Script node is a problem that may need to be resolved.
About VRU Error Checking

A special call variable VruStatus, allows you to check the result of the last IVR node (Send To VRU/Translation Route to VRU/Run VRU Script) that the ICM processed. The following table lists this variable’s values.

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>VRU_SUCCESS</td>
<td>The last VRU node was successful.</td>
</tr>
<tr>
<td>1</td>
<td>VRU_ERROR</td>
<td>The last VRU node failed because of a routing or configuration error.</td>
</tr>
<tr>
<td>2</td>
<td>VRU_TIMEOUT</td>
<td>The last Send To VRU or Translation Route to VRU node failed because the routing client did not respond within 20 seconds or the last Run VRU Script node failed because the timeout limit defined for the script expired.</td>
</tr>
<tr>
<td>3</td>
<td>VRU_ABORTED</td>
<td>The last VRU node did not complete because the caller hung up or was otherwise lost. (Because this causes the routing script to terminate immediately, this value is never seen.)</td>
</tr>
<tr>
<td>4</td>
<td>VRU_DIALOG_FAILED</td>
<td>The last VRU node failed because communication with the VRU ended unexpectedly.</td>
</tr>
<tr>
<td>5</td>
<td>VRU_SCRIPT_NOT_FOUND</td>
<td>The VRU failed because the referenced VRU script was not found in the ICM configuration.</td>
</tr>
</tbody>
</table>

How to Configure Routing and Administrative Scripts

After you have completed your ICM configuration, you can write *routing scripts* and *administrative scripts*:

- A *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 *administrative script* runs periodically to perform a task, such as setting variables.

You create, maintain, and monitor ICM scripts using the ICM Script Editor.

For Information On:  
Creating ICM scripts
Designing scripts for IPCC using the ICM Script Editor

See:  
ICM Configuration Guide for Cisco ICM Enterprise Edition
ICM Scripting and Media Routing Guide for Cisco ICM/IPCC Enterprise & Hosted Editions
Chapter 6: Installing and Configuring Cisco ICM for IPCC Enterprise

How to Configure ICM for IPCC Enterprise

For Information On:

Planning scripts for your IPCC reporting needs

Creating scripts for Outbound Option

See:

Reporting Guide for Cisco IPCC Enterprise & Hosted Editions

Outbound Option Setup and Configuration Guide for Cisco ICM/IPCC Enterprise & IPCC Hosted Editions

Outbound Option User Guide for Cisco ICM/IPCC Enterprise & IPCC Hosted Editions
Installing and Configuring Outbound Option for IPCC Enterprise

Outbound Option is a feature of ICM that provides outbound dialing functionality along with the existing inbound capabilities of ICM. 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.

About Outbound Option Installation and Initial Configuration

You install Outbound Option as an optional feature during ICM installation. Installation and initial configuration tasks for Outbound Option include:

- Enabling Outbound Option on ICM Components
- Installing the Outbound Option Dialer
- Creating the Outbound Option Private Database
- On the MR PG, creating a PIM for Outbound Option
- Configuring CallManager for Outbound Option
- Configuring the dialer
- Configuring Outbound controls for CTI desktop tools

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

About Outbound Campaigns

Once Outbound Option has been installed and configured you can begin creating outbound dialing campaigns. Outbound Option as an optional feature during ICM installation. Instructions for creating and managing outbound campaigns, and for writing scripts for use with Outbound Option, are provided in the Outbound Option User Guide for Cisco ICM/IPCC Enterprise & IPCC Hosted Editions.
About Outbound Campaigns
Installing and Configuring Cisco CVP for IPCC Enterprise

This chapter describes how to install and configure Cisco CVP for the IPCC Enterprise. Follow the instructions in this chapter if you are using CVP (as opposed to IP IVR) for queuing in your IPCC system. (If you are deploying IP IVR instead of CVP, refer to Chapter 5, “Installing and Configuring Cisco IP IVR for IPCC Enterprise.”)

It contains these sections:

- About CVP, page 8-1
- How to Install CVP for IPCC Enterprise, page 8-2
  - About CVP Installation Prerequisites, page 8-2
- How to Configure CVP for IPCC Enterprise, page 8-3
  - How to Configure the Application Server, page 8-3
  - How to Configure the Voice Browser, page 8-4
  - How to Set up Cisco Gateways/Gatekeepers to Interact with CVP, page 8-5
  - How to Update Cisco Listener and Alarm Tracker to Support SDDSN, page 8-7
  - How to Set up Cisco ICM software to Interact with CVP, page 8-7
  - How to Configure the Dynamic Routing Client, page 8-8

Related Documentation

The following additional Cisco documents provide additional information on the installation/configuration tasks described in this chapter:

- Cisco Customer Voice Portal (CVP) Installation Guide
- Cisco Customer Voice Portal (CVP) Configuration and Administration Guide

About CVP

Cisco Customer Voice Portal (CVP) can be deployed in the IPCC Enterprise system to provide IVR queuing and call treatment.

This guide provides basic information for configuring CVP for IPCC Enterprise. The exact manner in which you configure CVP depends on the deployment model of CVP that you are using for your system. For more detailed information on configuring CVP in your deployment model, refer to Cisco Customer Voice Portal (CVP) Administration and Configuration Guide.
How to Install CVP for IPCC Enterprise

Step-by-step installation instruction for CVP are included in the _Cisco Customer Voice Portal (CVP) Installation Guide._

When you install CVP, you install these components:

- Voice Browser
- Application Server
- System Media Files
- Standalone Distributed Diagnostics and Service Network (SDDSN) software and updates
- CVP Online Help
- Voice Browser Administration

If you are deploying an IPCC Enterprise _laboratory_ system, you can install all of these components on a single machine and must install all components at the same time. If you do not install all components and later decide to add a component, you must uninstall the existing CVP software and perform a complete re-install.

If you are deploying an IPCC Enterprise _production_ system, you can install individual components on different machines. To maximize performance, do not install the Voice Browser or Application Server on the Media Server, to which you copy System Media Files.

Tip

When installing CVP, record the user name and password that you enter on the Username and Password screen. You need to enter this user name and password combination when configuring the Application Server.

About CVP Installation Prerequisites

Before installing and configuring CVP, you must:

<table>
<thead>
<tr>
<th>CVP Installation Prerequisite</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Cisco CallManager</td>
<td>On CallManager, you must have configured the CVP Voice Browser as a Gateway on CallManager.</td>
</tr>
<tr>
<td>Install Cisco ICM software</td>
<td></td>
</tr>
<tr>
<td>and the PG containing the VRU</td>
<td></td>
</tr>
<tr>
<td>PIM(s).</td>
<td></td>
</tr>
</tbody>
</table>
How to Configure CVP for IPCC Enterprise

After installation, CVP must be configured for integration with IPCC. The following table lists the configuration tasks required to CVP in an IPCC Enterprise deployment. These tasks should be performed in the order listed. Instructions for each are included later in this section.

<table>
<thead>
<tr>
<th>CVP Configuration Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure the Application Server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Configure the Voice Browser.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Set up Cisco Gateways/Gatekeepers to interact with CVP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Define CVP Voice Browser as a gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Update Cisco Listener and Alarm Tracker software to support SDDSN.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Set up Cisco ICM software to interact with CVP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Optionally, configure CVP to use the Dynamic Routing Client feature</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How to Configure the Application Server

The Application Server processes IVR messages to the ICM software and sends VXML messages to the Voice Browser.

Tip

The VRU Port Connection value that you enter in step 10 must match the configuration value on the PG with VRU PIM.

To configure the Application Server:

1. Choose Start > Programs > Cisco Internet Service Node > Application Server > Application Administrator. The Enter Network Password dialog box opens.
2. Log in as the Windows 2000 Administrator, using the same user name and password that you entered when installing CVP. If the information is not exactly the same as the information provided during installation, the Application Server will not configure properly. The Application Administration Main Menu opens.
3. Click Call Definition. The Call Definition page opens.
4. Click one of the Group Number links. The Port Group Configuration (ID from ICM / New Call) page opens. Click:
   - **Group Number 100 / New Call** if you want to define call parameters for post-routing calls.
   - **Group Number 200 / ID from ICM** if you want to define parameters for translation routing.
5. Use the Initial Port and Last Port fields to specify a range of virtual ports for the Group Number.
The Application Server will not start up if you do not define any ports. Also, the number of ports you define determines the number of calls that can be processed simultaneously. Setting a large number of ports will impact system performance, even if the number of actual calls is not large.

6. Click **Update**. The changes take effect immediately.
7. Click **Return to Main Menu**.
8. Click **ICM** if you need to change the default VRU port setting. The ICM Subsystem Configuration page opens.
9. Specify a VRU Connection Port value. This is the TCP/IP socket number the Application Server will use to receive messages from the ICM PG with the VRU PIM. This setting must match the ICM PG with VRU PIM setting.
10. Click **Update** and then **Return to Main Menu**.
11. Click **Engine**. The Engine Status page opens.
12. Click **Log Configuration**. The Log Configuration page opens.
13. Use the SDDS section to specify settings to be used by Alarm Tracker process.
14. Scroll down and click **Update**. Changes to SDDS configuration take effect immediately.
15. Click **Status**. The Engine Status page opens.
16. To enable the auto-refresh feature, click the check box and specify how often the page should refresh.
17. Click **Start** and then **Yes** in the confirmation box that opens. The Application Server status changes to RUNNING and a green light appears, indicating that all subsystems are running and the Application Server is ready to accept calls.
18. Choose **File > Close** to close the Application Administrator window. The Application Server remains running under the ICM Service Control.

### How to Configure the Voice Browser

The Voice Browser accepts H.323 VoIP calls, sends URL requests to the Application Server, and retrieves system prompts from the Media Server.

Before configuring the Voice Browser, ensure that it is running.

To configure the Voice Browser:

1. Choose **Start > Programs > Cisco Internet Service Node > Voice Browser > VB Admin**. A window containing a command line prompt (>>>>) opens.
2. Enter `setASList<NewValue>`, where `<NewValue>` is the base URL of the Application Server. The syntax for the base URL is `<AppServer>:8000/servlet/isn`, where: `<AppServer>` is the hostname or IP address of the machine running the Application Server. The default is localhost.
   
   :8000/servlet/isn is a fixed string that you must append to each name in the AppServerList. The string must begin with a colon [:].
   
   Examples:
   
   ```
   setASList localhost:8000/servlet/isn
   setASList "machine1:8000/servlet/isn machine2:8000/servlet/isn"
   ```
   
   The setASList command contains no spaces. The use of double quotes is required when defining multiple Application Servers.
3. If you want a call restarted from the beginning if there is an ICM or Application Server problem during the course of the call, enter `SetNewCallOnly on`.

Do not set this value to “on” if you expect any pre-routed calls to come to this Voice Browser. The CVP cannot restart pre-routed calls.

4. If IP transfers will be part of your configuration, enter `setGatekeeper<NewValue>`, where `<NewValue>` is the IP address for the Gatekeeper serving the Voice Browser.

You must shut down and restart the Voice Browser for this setting to take effect.

5. If you chose to install SSDSN and need to change the default settings, enter the following:

   `setSSDSN1<NewValue>`, where `<NewValue>` is the hostname or IP address of the first SSDSN instance. (Default <none>)

   `setSSDSN2<NewValue>`, where `<NewValue>` is the hostname or IP address of the second SSDSN instance. (Default: <none>)

   If there is only one SSDSN in service, SSDSN2Node should be set to the same node as SSDSN1Node.

6. Enter `q` to exit VB Admin.

---

### How to Set up Cisco Gateways/Gatekeepers to Interact with CVP

You must configure Gateway(s) and Gatekeeper(s) in order to properly route inbound calls (calls originating from the caller into CVP) and outbound calls (calls being transferred to an agent through CVP).

Depending on the CVP configuration being used, certain folders of files need to be copied from the CVP Application Server machine to the Gateway(s). Use Table 2-1 to determine which folder you need to copy for your system. The first three columns of the table define a possible combination of features in an CVP configuration:

- **Voice Browser.** Your CVP configuration would include an CVP Voice Browser when the CVP needs to queue calls or provide call transfer after an agent has answered the call.
- **CSS.** If your CVP configuration includes one or more Cisco Content Services Switches to provide enhanced failover and load-balancing capabilities between the Voice Gateways and the ASR/TTS Servers, HTTP Media Servers, and the CVP Application Servers.

  **Note**: When a CSS exists in the configuration, it must be used with **all** the Servers in the configuration.

- **Call Restart.** Your CVP configuration would include the Call Restart feature to restart a call in the event of an CVP Application Server failure in mid-call. The restarted call will appear to the ICM as just another new call.

  **Note**: The Call Restart feature can only be used when the CVP is a Type 5 or Type 6 Network VRU or when the CVP is the main routing client for the call. In configurations where a call is pre-routed by a NIC to an CVP (that is, the CVP is a VRU Type 2, 3, 7 or 8), the restart feature cannot be used.
Once you have determined the feature combination of your CVP configuration, open the folder and copy all files specified in the fourth column of the table below from the CVP Application Server machine to flash memory on the Gateway(s).

### CVP Feature Combinations

<table>
<thead>
<tr>
<th>Voice Browser?</th>
<th>CSS?</th>
<th>Call Restart?</th>
<th>Folder To Copy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td><code>&lt;basedir&gt;/ApplicationServer/Downloads/VB-CSS-CallRestart</code></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td><code>&lt;basedir&gt;/ApplicationServer/Downloads/VB-CSS-noCallRestart</code></td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td><code>&lt;basedir&gt;/ApplicationServer/Downloads/VB-noCSS-CallRestart</code></td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td><code>&lt;basedir&gt;/ApplicationServer/Downloads/VB-noCSS-noCallRestart</code></td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td><code>&lt;basedir&gt;/ApplicationServer/Downloads/noVB-CSS-CallRestart</code></td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td><code>&lt;basedir&gt;/ApplicationServer/Downloads/noVB-CSS-noCallRestart</code></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td><code>&lt;basedir&gt;/ApplicationServer/Downloads/noVB-noCSS-CallRestart</code></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td><code>&lt;basedir&gt;/ApplicationServer/Downloads/noVB-noCSS-noCallRestart</code></td>
</tr>
</tbody>
</table>

Note: If your CVP configuration includes a CSS, you also need to copy the `askeepalive.txt` file from the root of the `Downloads` directory to the `Scripts` directory of the CSS switch.

If you are deploying CVP instead of IP IVR in your IPCC Enterprise system, you must define the CVP Voice Browsers as Gateways on Cisco CallManager. By defining the Voice Browsers as Gateways, Cisco CallManager can receive multiple calls from the Voice Browsers.

Note: The Gateway created on Cisco CallManager is similar to other Voice Gateways but does not support DNS lookups.

To define an Voice Browser as a Gateway:

1. In Cisco CallManager Administration, select Device > Gateway.
2. Click Find. Cisco CallManager lists any Gateways that are currently registered.
3. If your Voice Browser is not listed, click Add a New Gateway and specify the following:
   - Gateway Type. H.323 Gateway.
   - Device Protocol. H.225
4. Click Next.
5. Specify the following:
Chapter 8 Installing and Configuring Cisco CVP for IPCC Enterprise

How to Configure CVP for IPCC Enterprise

- **Device Name.** Voice Browser IP address.
- **Description.** Voice Browser IP address (or other identifying text).
- **Device Pool.** Default.
- **Calling Party.** Originator.
- **Presentation Bit.** Allowed.
- **Gatekeeper Name.** IP address of Gatekeeper.

6. Click **Insert.**

How to Update Cisco Listener and Alarm Tracker to Support SDDSN

Cisco Listener and AlarmTracker software (part of the Remote Monitoring Suite) needs to be updated with support files for SDDSN. You do this by installing the CVP component called “Update External SDDSN Components” on any machine that runs Listener or AlarmTracker.

To update external SDDSN components

1. From the installation CD, run **SETUP.EXE.**
2. On the **Welcome** screen, click **Next.**
3. On the **Copyrights** screen, click **Next.**
4. On the **CVP License Agreement** screen, click **Yes.**
5. On the **Choose Destination Location** screen, specify the drive and directory where the software will be installed:
   - Click **Next** to accept the default location (C:\Cisco\ISN).
   - Click the **Browse** button, select an alternate location, and then click **Next.**

     **Note** All CVP components you select will be installed to subfolders under the destination location.

6. On the **Install Cisco CVP Components** screen, select the **Update External SDDSN Components** option to install updates to components external to CVP, such as Cisco’s Listener and AlarmTracker. These updates make it possible for the components to process CVP-based event messages.
7. Click **Next.**
8. On the **Start Copying** files screen, click **Next.**
9. On the **CVP Setup Complete** screen and click **Finish.**

How to Set up Cisco ICM software to Interact with CVP

There are several “one time only” steps you need to take to enable interaction between NAM/ICM and CVP software:

- Determine what CVP Network VRU types you need to define
- Define an CVP Network VRU
- Set the Enable Expanded Call Context option
- Define expanded call context (ECC) variables for CVP
How to Configure CVP for IPCC Enterprise

Chapter 8 Installing and Configuring Cisco CVP for IPCC Enterprise

How to Configure CVP for IPCC Enterprise

- Define the default Network VRU
- Configure the Peripheral Gateway (PG) for the CVP

Note For more information, see the “CVP Deployment Options” section in the Cisco Customer Voice Portal (CVP) Configuration and Administration Guide.

How to Configure the Dynamic Routing Client

When ICM uses the Translation Route to VRU method to route a call to a type 2 SCI VRU, the VRU becomes the new routing client for the call. This means that the next Connect message is sent to the VRU to connect the call (to an agent, for example). The dynamic routing client feature is required to allow ICM to make a subsequent network transfer using the new VRU routing client.

Dynamic routing client capability is required for the following call scenarios:

- Receiving a call on a converged enterprise network after a carrier pre-route using CVP (release 2.1 and later) to control the call.
- Using pre-routing for load balancing purposes before the call is sent to an CVP-controlled network with call context and cradle to grave reporting capabilities.
- Supporting Outbound Option for Hosted IPCC where a shared Network VRU is used for providing announcements to targeted phones/answer machines.

In an environment where the routing client is not capable of Network Transfer, all the pre-route calls must be transferred to CVP via Translation Route To VRU to take advantage of the network transfer feature.

To configure CVP as a dynamic routing client:

1. Configure the CVP machine used for Dynamic Routing Client like any other, with the following exceptions:
   - In ICM Configuration Manager > Network VRU Explorer, define the machine as a Type 2 VRU.
   - In ICM Configuration Manager > PG Explorer, on the Routing Client tab, de-select Network Transfer Preferred for this peripheral.
   - In CVP AppAdmin > Call Definitions > Select Group 200 > Add New DNIS, add each Translation Route DNIS.

2. Size and configure the network appropriately.
   If the CVP machine resides in a different location than the CallManager cluster initiating the calls, WAN bandwidth is a consideration because the prompts are played G.711 from the CVP machine. Where possible, the CVP should be co-located with the CallManager to eliminate these bandwidth requirements.

3. Define a gateway device in CallManager for the CVP machine.
   In CallManager Administration, select Device > Gateway and define an H.323 gateway using the CVP IP address. You must check the “Media Termination Point Required” check box.

4. Configure MTP resources according to CallManager instructions for the type of MTP that you have selected to use (software or hardware).

5. Configure labels for the dynamic routing client.
   In ICM Configuration Manager, the routing target (the network VRU, device targets, services, etc.) must have labels configured for the type 2 VRU as routing client.
For information on scripting for Translation Route to VRU, see the *ICM Scripting and Media Routing Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*. For information on deploying a dynamic routing client with Outbound Option, see the *Outbound Option User Guide for Cisco ICM/IPCC Enterprise & IPCC Hosted Editions*. 

---

**Note**
CHAPTER 9

Installing Agent and Supervisor Desktops for IPCC Enterprise

You can deploy either Cisco CTI OS or Cisco Agent Desktop/Cisco IPCC Supervisor Desktop in the IPCC Enterprise system to provide agent and supervisor desktops. This chapter provides information on installing these options for IPCC Enterprise.

It contains these sections:

- About Agent and Supervisor Desktops for IPCC Enterprise, page 9-1
- About Agent and Supervisor Desktop Installation Prerequisites, page 9-2
- About Agent and Supervisor Desktop Installation Tasks, page 9-3
- How to Install the CTI OS Server, page 9-3
- How to Install and Configure CTI OS Desktops, page 9-5
- How to Install and Configure the CAD Agent and Supervisor Desktops, page 9-7
- How to Start CTI OS Services After Installation, page 9-9

Note

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

Related Documentation

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

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

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 includes the Desktop Administrator, Agent Desktop, and Supervisor Desktop.

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 either on a Peripheral Gateway (PG) or on a CTI Gateway (CG) machine. 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 desktop packages are supported by the CTI OS software. CTI OS provides an object-oriented software development toolkit for development and deployment of CTI applications. CTI OS is installed on the ICM CTI server.

### About Agent and Supervisor Desktop Installation Prerequisites

The following table lists the installation/configuration tasks required to CTI OS in an IPCC Enterprise deployment. These tasks should be performed in the order listed. Instructions for each are included later in this section:

<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 or CVP</td>
<td></td>
</tr>
<tr>
<td>Install and configure ICM</td>
<td></td>
</tr>
</tbody>
</table>

### About CTI OS Silent Monitor Feature Prerequisites

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 to the supervisor’s computer. The supervisor listens to the call through the sound card on his/her computer, not the phone.

- If the agent is using a hard phone, connect the agent’s computer to the second port on the agent’s phone to forward the agent’s voice traffic to the supervisor.
- If the agent is using Media Termination, the supervisor must have a hard phone connected to his/her computer in order to use Silent Monitor for that agent.

**Note**

For more information and instructions on configuring the Silent Monitor feature, see the *CT IOS System Managers Guide.*
About Agent and Supervisor Desktop Installation Tasks

The following table lists the configuration tasks required to CTI OS Server and Agent/Supervisor desktops in an IPCC Enterprise deployment. These tasks should be performed in the order listed. Instructions for each are included later in this section.

<table>
<thead>
<tr>
<th>Desktop Installation Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install and configure CTI OS Server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Install CTI OS Agent and Supervisor desktops, OR install CAD Agent and Supervisor Desktops</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Start CTI OS Services</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How to Install the CTI OS Server

CTI OS incorporates the CTI OS Toolkit, Agent Desktop, Supervisor Desktop and Client Interface Library. Complete the CTI OS related configuration on the ICM software. Step-by-step installation instructions for CTI OS are included in the Cisco ICM CTI OS System Manager’s Guide.

- Create a user for the ODBC File Data Source Name.
- Create and configure an ODBC file Data Source Name
- Install the CTI OS Supervisor Desktop
- Install the CTI OS Agent Desktop
- Start the CTI OS Service

How to Create a User for ODBC File Data Source Name

When configuring CTI OS, you create and configure an ODBC file Data Source Name (DSN) to store information about a database connection in a file. Before creating the DSN, configure a user for ODBC.

To configure a user for ODBC, complete the following steps:

1. On the ICM Logger, select Start > Programs > Microsoft SQL Server > Enterprise Manager.
2. In the Enterprise Manager window, expand Microsoft SQL Server > SQL Server Group > Sprawler server name > Databases > ICM side A database > Users.
4. From the Login name drop-down list, select New. The SQL Server Login Properties- New Login window opens.
5. Select the General tab. Enter a name for the new user.
6. Select the Windows Authentication option.
7. Do not enter a password.
8. From the default Database drop-down menu, select ICM side A Database.
9. Click OK. An error message indicating that the user has not been granted access opens.
10. Click Yes to proceed. The Database User Properties- New User dialog box opens.
11. From the Login name drop-down list, select the name of the new user that you just created.
12. Check the db_datareader permission.
13. Click OK.
14. Close the SQL Server Enterprise Manager.

How to Create and Configure an ODBC file Data Source Name

A file Data Source Name (DSN) stores information about a database connection in a file. The file has the extension .dsn and by default is stored in the $Program Files$Common files$ODBC$Data Sources directory. The CTI OS Server install process prompts for the file DSN and creates the appropriate registry keys.

Tip
Record the name of the File DSN that you create in step 6. You need to enter this value when installing CTI OS Server.

To create and configure a new file DSN on a Microsoft Windows 2000 system:

1. On the ICM Logger, select Start > Programs > Administrative Tools > Data Sources (ODBC).
2. Select the File DSN tab.
3. Click Set Directory. A message opens asking you to confirm setting the default File DSN directory. Click Yes.
5. Select SQL Server driver from the driver list.
6. Click Next and enter a name for the File DSN you are creating.
   You will need to use this name when installing CTI OS Server.
7. Click Next and verify the information.
8. Click Finish.
9. On the next dialog box that opens, enter the description of the DSN file that you are creating and the name or IP address and description of the your SQL Server where the Logger database is installed.
10. Click Next.
11. Choose the SQL Server Authentication option and enter the Login ID for the user that you choose to access the database. Do not enter a password. The password field should be blank.
12. Click Next.
13. Select the Change the Default Database To check box and select the ICM side A database from the drop-down list. Accept the defaults for the other items.
14. Click Next and then click Finish.
15. Click Test Data Source and confirm that the test completed successfully. Click OK.
16. Verify the information in the dialog box that appears and click OK.
How to Install CTI OS Server

To install the CTI OS server, complete these steps:
1. From the Server directory on the CD, run Setup.exe.
2. Click Yes on the Software License Agreement screen.
3. If prompted for customer information, enter the current instance name. Click Next.
4. On the Destination Location screen, accept the default installation directory or click the Browse button to specify another directory. Click Next.
5. On the CTI Server Information dialog box, enter the name or IP address and the port number for your CTI Server. Click Next.
6. On the Peripheral Identifier dialog box, specify the following information:
   - Logical Name: A Logical Name for your peripheral.
   - Peripheral ID: The Peripheral ID associated with the CTI Server to which your system talks.
   - Peripheral Type: Set to IPCC/SoftACD.
7. Click Next.
8. On the ODBC Connection dialog box, browse to the primary (SideA) ODBC file DSN in the C:\Program Files\Common Files\ODBC\DataSources\ODBC file DSN. Click Next.
9. On the Peer CTI OS Server screen, check the Duplex CTI OS Install option in you want to install duplexed CTI OS Servers.
10. Click Install.
11. When the installation is complete, the Setup Complete dialog box appears. Click Finish.

How to Install and Configure CTI OS Desktops

How to Install the CTI OS Supervisor Desktop

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:
1. From the Install > CTI OS Client directory on the CTI OS CD, run Setup.exe.
2. Click Yes on the Software License Agreement screen.
3. On the Destination Location screen, accept the default installation directory or click the Browse button to specify another directory. Click OK.
4. On the Select Components screen, select IPCC Supervisor Desktop. Click Next.
5. On the CTI OS Server Information screen, enter the name or IP address for your CTI OS Server. Accept the default Port number 42028. Click Next.

6. Click Next to start the installation.

7. 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.

8. 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.

9. When the installation of files is complete, Click Finish.

10. Reboot the machine to complete the installation.

---

**How to Install the CTI OS Agent Desktop**

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 your 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:

1. From the Install > CTI OS Client directory on the CTI OS CD, run Setup.exe.

2. Click Yes on the Software License Agreement screen.

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

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

5. On the CTI OS Server Information screen, enter the name or IP address for your CTI OS Server. Accept the default Port number 42028. Click Next.

6. Click Next to start the installation.

7. 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.

8. 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.

9. When the installation of files is complete, Click Finish.

10. Reboot the machine to complete the installation.
How to Install and Configure the CAD Agent and Supervisor Desktops

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><strong>Primary Directory Services</strong></td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</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>Host name / IP address</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>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</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>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>CallManager Database</td>
<td>CallManager version</td>
</tr>
<tr>
<td>Item</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Database login ID</td>
<td></td>
</tr>
<tr>
<td>Database password</td>
<td></td>
</tr>
<tr>
<td>IPCC SQL Logger Database</td>
<td></td>
</tr>
<tr>
<td>(Located on Central Controller)</td>
<td></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>Side A</td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Side B</td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>CTI Service Associated with CallManager</td>
<td></td>
</tr>
<tr>
<td>Peripheral ID</td>
<td></td>
</tr>
<tr>
<td>Side A</td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Side B</td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>CTI Service Associated with IP IVR</td>
<td></td>
</tr>
<tr>
<td>Peripheral ID</td>
<td></td>
</tr>
<tr>
<td>Side A</td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Side B</td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>CTI OS (Server 1)</td>
<td></td>
</tr>
<tr>
<td>Peripheral ID</td>
<td></td>
</tr>
<tr>
<td>Side A</td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Side B</td>
<td></td>
</tr>
<tr>
<td>Host name / IP address</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
</tbody>
</table>
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.

### How to Start CTI OS Services After Installation

The CTI OS Server runs as a Windows service on the host computer. The ICM Service Control application is an interface into the Windows service control manager, which starts and stops services.

To start the CTI OS Service:
1. On the CTI OS Server machine, open ICM Service Control.
2. Select CTI OS Service.
3. Click Start. Two process windows open, one for ctidriver and one for ctios server.
4. Check that both window title bars indicate that the processes are Active.

For detailed descriptions of these processes see the Cisco Agent Desktop (CAD) Installation Guide.
CHAPTER 10

Installing and Configuring Cisco Multichannel Components for IPCC Enterprise

This chapter describes how to install and configure Cisco multichannel software for the IPCC Enterprise system in both production and laboratory environments.

It contains these sections:

- About IPCC Enterprise Multichannel Components, page 10-2
- How to Install Multichannel Components for IPCC Enterprise, page 10-2
  - About Multichannel Installation Prerequisites, page 10-3
- How to Configure Multichannel Components for IPCC Enterprise, page 10-3
  - About Multichannel Configuration Tasks, page 10-3
  - About ICM Configuration for Multichannel Components, page 10-4
  - How to Configure Media Routing Domains, page 10-7
  - How to Configure Application Instances, page 10-8
  - How to Establish Administration Connections, page 10-8
  - How to Set ECC (Expanded Call Context) Variables, page 10-10
  - How to Write ICM Routing Scripts for Multichannel Options, page 10-11
  - How to Configure Cisco Media Blender for ICM Integration, page 10-12
  - How to Configure Cisco E-Mail Manager for ICM Integration, page 10-12

Related Documentation

The following additional Cisco documents provide additional information on the installation/configuration tasks described in this chapter:

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

IPCC multichannel components include the Cisco Collaboration Server, Cisco Media Blender, The Dynamic Content Adapter, 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 ICM CallRouter via the MR-PG, and the CallRouter 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.

Optionally, the Cisco Dynamic Content Adapter (DCA) can also be deployed with CCS. The DCA is an intelligent Web proxy caching server that allows the Collaboration Server users to share secure, personalized, live, interactive, and transactional Web content.

About Cisco E-Mail Manager

Cisco E-Mail Manager (CEM) manages high volume 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 ICM CallRouter via the MR-PG, and the CallRouter routes the request to an available agent.

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
- Dynamic Content Adapter Installation and Integration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions
About Multichannel Installation Prerequisites

Before installing and configuring multichannel components, you must:

<table>
<thead>
<tr>
<th>Multichannel Installation Prerequisite</th>
<th>Installation Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install and configure ICM software components, including the CallRouter, Logger, Admin Workstation, and HDS.</td>
<td></td>
</tr>
<tr>
<td>Install and configure the ICM MR PG.</td>
<td></td>
</tr>
<tr>
<td>For the Dynamic Content Adapter and Cisco Media Blender, install and configure Cisco Collaboration Server.</td>
<td></td>
</tr>
</tbody>
</table>

How to Configure Multichannel Components for IPCC Enterprise

After installation, multichannel components must be configured for integration with ICM, which in turn integrates them with the IPCC Enterprise.

About Multichannel Configuration Tasks

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

<table>
<thead>
<tr>
<th>Multichannel Configuration Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure Media Routing Domains</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Configure Application Instances</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Establish Administration Connections</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Set ECC (Expanded Call Context) Variables</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Write ICM Routing Scripts for multichannel Options</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Configure Cisco Web Collaboration Server for ICM Integration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 10 Installing and Configuring Cisco Multichannel Components for IPCC Enterprise

How to Configure Multichannel Components for IPCC Enterprise

Note

The Dynamic Content Adaptor requires no integration configuration with ICM. It’s relationship with ICM is established through its integration with Cisco Collaboration Server. See the Dynamic Content Adapter Installation and Integration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions for instruction on integrating the DCA with Cisco Collaboration Server.

About ICM Configuration for Multichannel Components

Before configuring ICM software for multichannel options, you must understand these concepts:

- About Media Routing Domains and Media Classes, page 10-5
- About Media Routing Domains and Media Classes, page 10-5
- About Multichannel Agents, page 10-5
- About Application Instances, page 10-6
- About Multichannel Skill Groups, page 10-7
- About Multichannel Skill Groups, page 10-7
- About Universal Queue and Multichannel Routing Scripts, page 10-7

About Media Routing Peripheral Gateways

To route to any multichannel or Outbound Option requests, you must establish a Media Routing Peripheral Gateway (MR-PG). The MR-PG accepts and translates information in requests initiated from the Web or through E-Mail into information that ICM routing scripts can understand. MR-PGs support multiple media routing applications by placing multiple, independent Peripheral Interface Managers (PIMs) on a PG platform. For IPCC, configure PIMs for E-Mail Manager, Web collaboration, and Outbound Option.

When ICM software receives a new task request from the application, ICM runs a pre-defined ICM script to determine how to handle the task. As a result of the execution of the ICM script, ICM 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 ICM. ICM 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 ICM determined best available agent that has the matching skill within the enterprise.

The MR-PG must be set up as a Network VRU; you must create a Media Routing Network VRU when you want to route multichannel requests with IPCC Enterprise.

The MR-PG is required in addition to the CallManager and VRU PGs used in your IPCC Enterprise system. See Chapter 6, “Installing and Configuring Cisco ICM for IPCC Enterprise” for instructions on setting up and installing the MR PG.
Note  You can use ICM Web Collaboration software to route Web Callback and Delayed Callback requests. If you do so, you must associate a label with the device target (phone) to which the Web Callback and Delayed Callback requests are routed.

About Media Routing Domains and Media Classes

ICM software uses Media Routing Domains (MRDs) to organize how requests for different media are routed. An MRD is a collection of skill groups and services that are associated with a common communication medium. ICM software uses an MRD to route a task to an agent who is associated with a skill group and a particular medium. Before you can configure your applications to use the ICM as a routing engine, you must establish MRDs in the ICM software. These MRDs must have unique IDs across the enterprise.

You establish MRDs using the ICM Configuration Manager. Once MRDs are established in ICM software, you must enable them in the multichannel software.

A Media Class describes the type of requests you want to set up for routing on the ICM software. These Media Classes are automatically set up when you install ICM software:

- 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

You can create multichannel agents using either the ICM Configuration Manager UI or the Administration interface for the multichannel software. The following table explains why creating multichannel agents using the multichannel software is the preferred method for agent creation.

<table>
<thead>
<tr>
<th>If you create agents using the ICM Configuration manager:</th>
<th>If you create agents using the multi-media software:</th>
</tr>
</thead>
<tbody>
<tr>
<td>You must create a person record and an agent record in ICM software.</td>
<td>Agent and person records are automatically created in both the multichannel software’s database and the ICM database.</td>
</tr>
<tr>
<td>You must enable agents in the associated multi-media software.</td>
<td>You do not need to create a person or agent record in the ICM Configuration Manager.</td>
</tr>
<tr>
<td>For example, imagine that you create an agent using the ICM Configuration Manager and you want that agent to be able to handle Web-initiated Single-session chat, Multi-session chat, and/or Blended Collaboration requests. To do so, you must use the Collaboration Administration desktop to <em>enable</em> the agent on the Collaboration Server.</td>
<td></td>
</tr>
</tbody>
</table>
When you create an Agent record, you have the option of associating with an existing Person record. If you do not associate the Agent record with an existing Person record, a new Person record is automatically created when you create the agent.

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.

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

About Voice and Non-Voice 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

In most cases, the CallManager PG (set up with your initial IPCC installation) tracks and records the state and activity of all voice and non-voice agents. However, you can configure a Non-Voice PG rather than a CallManager PG to monitor state and activity of agents who are non-voice agents. This is optional, and not necessary if you already have a CallManager PG configured for Voice agents.

About Application Instances

An application instance represents a single software application that has been integrated with ICM software. Each Collaboration server or E-Mail server in your enterprise must be configured as a separate application instance in the ICM software. For example, if your enterprise uses three Collaboration servers, you must configure three application instances in the ICM software.

You set up application instances through the ICM Configuration Manager. For each multichannel option that you want to use, you must establish an application ID and application key (password) that identifies the multi-media feature you want to implement. Once you have configured the application instance on the ICM, 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></td>
</tr>
<tr>
<td>Application key for Collaboration</td>
<td></td>
</tr>
<tr>
<td>Application instance for E-Mail</td>
<td></td>
</tr>
<tr>
<td>Application key for E-Mail</td>
<td></td>
</tr>
</tbody>
</table>
About Multichannel Skill Groups

In a multichannel configuration, skill groups are media 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 CallRouter 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 ICM Configuration Manager 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>ICM Configuration Manager</td>
</tr>
<tr>
<td>Multi-session chat, Single-session chat, Blended Collaboration</td>
<td>ICM Web Collaboration option</td>
</tr>
<tr>
<td>E-Mail</td>
<td>ICM E-Mail Manager option</td>
</tr>
</tbody>
</table>

About Universal Queue and Multichannel Routing Scripts

Universal Queue is a feature of the ICM architecture that places multiple media types under the routing control of ICM software. ICM 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, ICM software 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 ICM picks the agent.

The CallRouter 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 Media Routing Domains

You must establish Media Routing Domains (MRDs) for each multi-media class that your IPCC Enterprise System will support. Valid media classes are:

- Multi-session chat
- Single-session chat
- Blended Collaboration
- E-Mail
- Voice
How to Configure Multichannel Components for IPCC Enterprise

Note

A MRD for the Voice media class is installed by default with your IPCC software. You do not need to create a MRD for the Voice media class.

To create each MRD that your site will use:
1. Start the ICM Configuration Manager and select **Tools > List Tools > Media Routing Domain List**.
2. Click the **Retrieve** button and then the **Add** button to display the Attributes tab.
3. Enter the following information:
   - **Name**: Enter the enterprise name of the MRD.
   - **Media Class**: Use the drop-down list to select the media class for the integrated application. The MR domain ID is automatically generated when you save the MRD.
4. After entering the required fields, save the configuration and close the window.
5. Repeat this procedure to add an MRD for each media class that your system will support.

How to Configure Application Instances

You configure application instances for each installation of a multi-media feature in your configuration. For instance, if you have installed two Collaboration servers and one E-Mail server, you must set up three Application Instances.

Tip

Record the application name and key created in step 3. You need to enter these values on the multichannel software applications.

To configure application instances:
1. From the ICM Configuration Manager, select **Tools > List Tools > Application Instance List**. The Application Instance List window displays.
2. Click **Retrieve** and then **Add** to display the Attributes tab.
3. Enter the following information:
   - **Name**: The enterprise name for the application instance.
   - **Application key**: This is the password that the integrated application will use to be identified by ICM software.
   - **Application type**: Available options are: Cisco_Collaboration_Server and Cisco_Email_Manager.
   - **Permission Level**: Select the permission level from the drop-down list.
4. After entering the required fields, save the configuration and close the window.
5. 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 ICM software and the multi-media software.
Connections between the multi-media software and the ICM Administration workstation use Sun Microsystems 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 ICM 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 the ICM Admin Workstation, the Collaboration server, and the E-Mail Manager server.

The following image illustrates the screen in the ICM Admin Workstation, E-Mail software, and Collaboration software where you must enter RMI connection details.

To configure administration connections on the ICM, 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 three separate administration connections.

1. From the ICM Admin Workstation, select CMS Control.
2. Select the Application tab.
3. Click Add. The Application Connection Details dialog box displays.
4. Enter the application connection properties, using the form in About Multichannel Skill Groups, page 10-7. Complete this screen as follows

**ICM Distributor AW link.** Enter the link name on the ICM software. This can be any value, but must match the value you configure for “remote link name” in your multichannel applications. (Note that this name will be referred to as the “remote service name” in the multichannel application administration UIs).

**ICM Distributor AW RMI registry port.** Enter the RMI registry port number you want the ICM Distributor Admin Workstation.

**Note** To prevent conflicts with SQL Server 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.

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

5. Click **OK** twice. This restarts the Cms_Jserver on the Admin Workstation.

*Cisco Collaboration Server Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*
*Cisco Media Blender Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*
*Dynamic Content Adapter Installation and Integration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*
*Cisco E-Mail Manager Installation and Configuration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*

**How to Set ECC (Expanded Call Context) Variables**

Several ECC variables must be configured in the ICM Configuration Manager’s Expanded Call Variable List tool (for each integrated multichannel feature) in order to route multichannel requests.

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

- user.cisco.Category
- user.cisco.MessageKey
- user.cisco.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 Expanded Call Variable List tool in the ICM Configuration Manager to limit the user.cisco.cmb variable to 8 bytes and the user.cisco.cmb.callclass variable to 10 bytes to prevent ECC 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 ECC variables in your inmap file, or to ECC variables in ICM software, you must restart Cisco Collaboration for changes to take effect.

To configure ECC variables, complete these steps:
1. Ensure that the ECC Variables are enabled, using the System Information Tool (under Miscellaneous Tools).
2. Start the ICM Configuration Manager and select Tools > List Tools > Expanded Call Variable List.
3. Click Retrieve to activate the Add button.
4. Click Add.
5. Fill in the required data fields on the right side of the window.
6. Click Save.

Cisco ICM Configuration Manager online help

How to Write ICM Routing Scripts for Multichannel Options

You must also write routing scripts that will route multichannel requests to appropriate agents. Once you’ve completed the Collaboration and/or E-Mail set up, you can write scripts to test routing of each media, and universal queue.

ICM Scripting and Media Routing Guide for Cisco ICM/IPCC Enterprise & Hosted Editions

How to Configure Cisco Web Collaboration Server for ICM 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 ICM software.

Note
You do not need to perform any specific tasks to integrate Cisco Dynamic Content Adapter with the ICM software. Configure DCA as described in the Cisco Dynamic Content Adapter documentation set if you choose to deploy DCA as part of the Web Collaboration Option.

To configure Collaboration Server for ICM integration:
1. Identify the Collaboration application instance.
2. Run the Integrate with ICM wizard. This wizard walks you through:
   - Defining the CCS application instance in an ICM-integrated configuration
   - Establishing an ICM Administration connection to the ICM Distributor Admin Workstation

The wizard also covers:
   - Enabling ICM Media Routing Domains
1. 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.

2. Enabling ICM Agent Peripherals. You must enable the peripherals that will track agent activity. In most cases, the agent peripheral is the CallManager PG. However, if you have established a non-voice agent PG, you must enable that in Collaboration Server as well.

3. Create queues.

4. Create agents and skill groups.

5. Configure HTML callforms to gather caller information.

6. Periodically synch and verify the Collaboration Server database with the ICM database.

How to Configure Cisco Media Blender for ICM Integration

To configure ICM Media Blender for ICM integration:

1. Configure the ciscoccti.properties file.

2. Configure the firewall gateway.

How to Configure Cisco E-Mail Manager for ICM Integration

Setting up E-Mail 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 ICM software:

To configure E-Mail Manager for ICM integration:

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 and application key
   - The ICM Media Routing Domain
   - The Administration Connection name to the ICM Distributor Admin Workstation (Use the form included in the section About Multichannel Skill Groups, page 10-7 for Administration Connection information.)
   - RMI Service Name and Registry port for E-Mail Manager software
   - RMI Service Name and Registry port for the ICM Distributor AW
   - Host Name of the ICM Administration Workstation

2. Establish an ICM Administration connection to the ICM Distributor Admin Workstation.

3. Enable ICM Media Routing Domains.
4. Enable ICM Agent Peripherals--You must enable the peripherals that will track agent activity. In most cases, the agent peripheral is the CallManager PG. However, if you have established a non-voice agent PG, you must enable that in Collaboration Server as well.

5. Configure ICM Routing skill groups and agents.

6. Configure rules to route messages to ICM Routing skill groups.

7. Periodically verify and synch the E-Mail Manager database with the ICM database.

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
How to Configure Multichannel Components for IPCC Enterprise
Configuring Reporting for IPCC Enterprise

This chapter describes tasks required to configure reporting for your IPCC Enterprise system. Refer to the Reporting Guide for Cisco IPCC Enterprise & Hosted Editions for additional information regarding IPCC Enterprise reporting.

It contains these sections:

- About Reporting Configuration Prerequisites, page 11-2
- About IPCC Reporting Configuration Tasks, page 11-2
- How to Configure Agent Reporting, page 11-2
- How to Configure Service Levels, page 11-3
- How to Configure Bucket Intervals, page 11-4
- How to Configure IVR Applications, page 11-5
- How to Configure Short Calls, page 11-6
- About Other Reporting Setup Options, page 11-7

Related Documentation

The following additional Cisco documents provide additional information on the installation/configuration tasks described in this chapter:

- Reporting Guide for Cisco IPCC Enterprise & Hosted Editions
- ICM Configuration Manager online help
- ICM Scripting and Media Routing Guide for Cisco ICM/IPCC Enterprise & Hosted Editions

How to Configure Reporting for IPCC Enterprise

Most of the setup required for IPCC Enterprise reporting is accomplished in the course of normal IPCC component configuration described in earlier chapters. This chapter lists additional required and optional reporting configuration tasks beyond those covered earlier. The tasks described in this chapter are all performed using the ICM Configuration Manager on an ICM Admin Workstation.
About Reporting Configuration Prerequisites

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

<table>
<thead>
<tr>
<th>Reporting Configuration Prerequisite</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install and configure CallManager</td>
<td></td>
</tr>
<tr>
<td>Install and configure ICM</td>
<td>On the ICM configuration, you must have:</td>
</tr>
<tr>
<td></td>
<td>• Enabled Agent Reporting for the IPCC PG.</td>
</tr>
<tr>
<td></td>
<td>• Enabled Agent Event Detail for the IPCC PG.</td>
</tr>
<tr>
<td></td>
<td>• Created call types, agents and skill groups.</td>
</tr>
<tr>
<td>Install and configure IP IVR or CVP</td>
<td></td>
</tr>
<tr>
<td>Define all peripherals for your IPCC system</td>
<td></td>
</tr>
</tbody>
</table>

About IPCC Reporting Configuration Tasks

The following table lists the reporting configuration tasks required in an IPCC Enterprise system. These tasks should be performed in the order listed. Instructions for each are included later in this section.

<table>
<thead>
<tr>
<th>Reporting Configuration Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure Agent Reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Configure Service Levels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Configure Bucket Levels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Configure IVR Applications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Optionally, modify Short Calls configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Optionally, modify other features that affect reporting</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How to Configure Agent Reporting

Your ICM system must be configured properly to enable agent reporting. To enable agent reporting you must:

- Enable Agent Reporting for the CallManager PG
- Specify the Admin Workstation Distributor for CallManager PIMs

How to Enable Agent Reporting for the CallManager PG

To enable agent reporting for the CallManager PG:

1. In the ICM Configuration Manager, select Tools > Explorer Tools > PG Explorer.
2. Click Retrieve.
3. Under each PG, select the CallManager PIM (peripheral Select) and perform these steps:
   a. Select the Distribution tab.
   b. Ensure that the **Enable Agent Reporting** and **Agent Event Detail** check boxes are selected.
   c. Click **Save**.

**How to Specify the Admin Workstation Distributor for CallManager PIMs**

You must specify the Admin Workstation to which agent information should be sent by the ICM router and logger. You do so by adding an entry for the appropriate Admin Workstation within the Agent Distribution list.

1. In the ICM Configuration Manager, select Tools > Explorer Tools > PG Explorer.
2. Click **Retrieve**.
3. Under each PG, select the CallManager PIM (peripheral Select) and perform these steps:
   a. Select the Distribution tab.
   b. Click **New**.
   c. In **Distributor Site Name**, enter the site name of the Admin Workstation to which the ICM router and logger should send agent information. This is the same name that is entered during AW distributor set up. If nothing is entered for the site name during installation, it defaults to the host name.
   d. Ensure that the **Enabled** check box is checked.
   e. Click **Save**.

**How to Configure Service Levels**

*Service Levels* allows you set and measure goals for answering calls. Service Level is configurable; that is you can define it in different ways, depending on the kind of information you want it to provide.

You define Service Levels for Call Types and Services. For Call Types, a system-wide Service Level must be defined. This can be overridden by local settings for specific Call Types. For Services, Service Level is defined only on individual Services. Note that in IPCC Enterprise service reporting is on IVR services only.

System defaults for Service Level configuration are as follows:

- Call Type Service Level Threshold: 20
- Call Type Service Level Type: 
- Service Service Level Threshold: -1
- Service Service Level Type: Default

**How to Set the System Service Level for Call Types**

To set the Call Type Service Level for your IPCC Enterprise system:

1. In the ICM Configuration Manager, select Tools > Miscellaneous Tools > System Information.
2. Specify a value for the **Service Level Threshold**, in seconds.
3. Select the **Service Level Type**.
4. Click Save.

**How to Set Service Levels for Call Types**

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

1. In the ICM Configuration Manager, select Tools > List Tools > Call Type List.
2. Click Retrieve.
3. Select the Call Type whose Service Level you want to set.
4. Specify a value for the Service Level Threshold, in seconds.
5. Select the Service Level Type.
6. Click Save.

**How to Set the Service Levels for Services**

If desired, you can also specify the Service Level for specific Services:

1. In the ICM Configuration Manager, select Tools > Explorer Tools > Service Explorer.
2. Select the Peripheral whose Services you want to modify.
3. Enter any desired filter data. Click Retrieve.
4. Select the Service whose Service Level you want to set.
5. Specify a value for the Service Level Threshold, in seconds.
6. Select the Service Level Type.
7. Click Save.

**How to Configure Bucket Intervals**

*Bucket Intervals* allow you to track data for calls abandoned or answered within specific time increments (e.g., 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, you should only modify Bucket Interval settings at specific time boundaries (e.g., 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 Define Bucket Intervals**

Before you can assign a Bucket Interval to the system or a particular Call Type, you must create its definition. To define a Bucket Interval:

1. In the ICM Configuration Manager, select Tools > List Tools > Bucket Intervals List.
2. Click Retrieve.
3. Click Add.
4. In the Add Name field, enter a name for the interval.
5. In the Upper Bounds fields, add up to nine successive increments to measure, in seconds.
6. Click Save.

How to Set the System Bucket Interval

To set the Bucket Interval for your IPCC Enterprise system:
1. In the ICM Configuration Manager, select Tools > Miscellaneous Tools > System Information.
2. From the Bucket Intervals list, select the interval you want to use.
3. Click Save.

How to Set Bucket Intervals for Call Types

If desired, you can also configure Bucket Intervals for specific Call Types. These will override the system level setting:
1. In the ICM Configuration Manager, select Tools > List Tools > Call Type List.
2. Click Retrieve.
3. Select the Call Type whose Bucket Interval you want to set.
4. From the Bucket Intervals list, select the interval you want to use.
5. Click Save.

How to Configure IVR Applications

There may be cases when a call is not queued, but instead sent to the agent directly (via the LAA Select node) from the IVR. You must ensure the IVR PG is configured correctly to ensure that such a call is considered answered at the IVR service rather than abandoned.

Note This configuration is only necessary if you are deploying IP IVR (as opposed to CVP) in your IPCC Enterprise system.

1. In the ICM Configuration Manager, select Tools > Explorer Tools > PG Explorer.
2. Click Retrieve.
3. Select the IP IVR peripheral.
4. In Configuration Parameter, insert /ASSUME_ANSWERED.
5. 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 can be configured for both Call Types and Services. Additionally, for Services, you can set different configurations for Abandoned Short Calls and Answered Short Calls.

Note

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

System defaults for Service Level configuration are as follows:
- Call Type Service Level Threshold: 20
- Call Type Service Level Type:
- Service Service Level Threshold: -1
- Service Service Level Type: Default

System defaults for Short Call configuration are as follows:
- Call Type Abandoned Call Wait Time: 15
- Service Abandoned Call Wait Time: 5
- Service Answered Short Calls Threshold: 0

How to Configure Short Calls for Call Types

For Call Types, you can configure Abandoned Short Calls only. Call Types do not allow support configuration for Answered Short Calls.

To configure Abandoned Short Calls for Call Types:
1. In the ICM Configuration Manager, select Tools > Miscellaneous Tools > System Information.
2. Set Abandoned Call Wait Time to a value, in seconds. This value indicates the length of calls to be considered abandoned. To not track abandoned calls, leave the field blank.
3. Click Save.

How to Configure Short Calls for Services

Short Calls for Services are configured on the PG.

How to Configure Abandoned Short Calls for Services

To configure Abandoned Short Calls:
1. In the ICM Configuration Manager, select Tools > Explorer Tools > PG Explorer.
2. Click Retrieve to retrieve the list of PGs.
3. Under a PG, select the peripheral that you want to modify.
4. Select the Peripheral tab.
5. Set Abandoned Call Wait Time to a value, in seconds. This value indicates the length of calls to be considered abandoned. This number must be the same that you set for the Abandon Call Wait Time on the Call Type. To not track abandoned calls, leave the field blank.

6. Click **Save**.

7. Repeat steps 3-5 for additional PGs/peripherals, as desired.

### How to Configure Answered Short Calls for Services

To configure Answered Short Calls:

1. In the ICM Configuration Manager, select Tools > Explorer Tools > PG Explorer.

2. Click **Retrieve** to retrieve the list of PGs.

3. Under a PG, select the peripheral that you want to modify.

4. Select the Advanced tab.

5. Set **Answered Short Calls Threshold** to a value (in seconds) less than your Service Level Threshold but greater than zero (see **How to Set the Service Levels for Services**, page 11-4).

6. Click **Save**.

7. Repeat steps 3-5 for additional PGs/peripherals, as desired.

### 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 **Reporting Guide for Cisco IPCC Enterprise & Hosted Editions** provides guidelines and details for setting up supervisory features.

#### About Agent Transfer and Conferencing

Call transferring and conferencing can be accomplished in two ways. The agent can manually transfer the call to another agent or conferences in another agent or party by dialing the recipient's extension directly. Or the agent can also use the Dialed Number Plan to access a routing script, designed specifically to handle transfer or conference calls.
The *IP Contact Center Enterprise Edition Reporting Guide* provides guidelines and details for setting up agent transfer and conferencing.
IPCC Enterprise Checklists and Worksheets

This appendix provides a compilation of the IPCC installation and configuration checklists and worksheets appearing in this guide. These can be used to guide you through an IPCC Enterprise deployment.

This appendix contains these sections:

- IPCC Enterprise Hardware Installation Tasks, page A-2
- IPCC Enterprise Component Software Installation Tasks, page A-3
- IPCC Enterprise Component Software Configuration Tasks, page A-6
- IPCC Enterprise Configuration Values Worksheets, page A-11
## IPCC Enterprise Hardware Installation Tasks

This section lists the basic order of IPCC component hardware installation. For hardware installation instructions, see the documentation packaged with each component.

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install the Media Convergence Server(s) for Cisco CallManager and IP IVR (if you are using IP IVR rather than CVP in your IPCC system).</td>
<td>Hardware and OS requirements for these servers are available from the Hardware Bill of Materials. Network architecture requirements are described in the <em>Cisco IP Contact Center Solution Reference Network Design Guide</em>.</td>
<td></td>
</tr>
<tr>
<td>2. Install the ICM, PG, CVP (if deploying), CT IOS, and Multichannel application servers</td>
<td>Hardware and OS requirements for these servers are available from the Hardware Bill of Materials. Network architecture requirements are described in the <em>Cisco IP Contact Center Solution Reference Network Design Guide</em>.</td>
<td></td>
</tr>
<tr>
<td>3. 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 <em>IPCC Compatibility Guide</em> for a list of supported IP Phones.</td>
<td></td>
</tr>
</tbody>
</table>
# IPCC Enterprise Component Software Installation Tasks

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

<table>
<thead>
<tr>
<th>Task</th>
<th>IPCC Installation Prerequisites</th>
<th>IPCC Installation Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install CallManager</td>
<td>There are no IPCC-specific installation prerequisites for CallManager.</td>
<td>There are no IPCC-specific installation instructions for CallManager.</td>
</tr>
</tbody>
</table>
| 2. Install IP IVR (if IP IVR will be used for queueing). | 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 JTAPI 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 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 ICM 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. See Chapter 5, “Installing and Configuring Cisco IP IVR for IPCC Enterprise” for instructions. |
<table>
<thead>
<tr>
<th>Task</th>
<th>IPCC Installation Prerequisites</th>
<th>IPCC Installation Notes</th>
</tr>
</thead>
</table>
| 3.   | Install ICM software, including the CallRouter, Logger, Admin Workstation, and Historical Data Server (HDS) database. | Install 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 a CallManager PG JTAPI user and associated the user with CTI Route Point(s) and CTI Port(s).  
- Enabled CTI for the CallManager PG user.  
Install IP IVR if your IPCC Enterprise system will use IP IVR for queueing. 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 | There are no IPCC-specific installation instructions for ICM. If you will be deploying the Outbound Option, see Chapter 6, “Installing and Configuring Cisco ICM for IPCC Enterprise” for instructions on enabling Outbound Option during ICM installation. |
<p>| 4.   | Install the System or Generic IPCC PG. | Before installing the Generic IPCC PG, you must configure it in ICM. |
| 5.   | Install JTAPI Client on the Generic or System PG. | Before installing the JTAPI Client, you must configure the Generic IPCC PG. |
| 6.   | Install the Media Routing PG (MR-PG) if deploying Multichannel options and/or Outbound Option. | Before installing the MR-PG, you must configure it in ICM. |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>IPCC Installation Prerequisites</th>
<th>IPCC Installation Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Install the CVP software (if CVP will be used for queueing). Install Cisco CallManager. On CallManager, you must have configured the CVP Voice Browser as a Gateway on Cisco CallManager. Install Cisco ICM software and the PG containing the VRU PIM(s).</td>
<td>If you are deploying an IPCC Enterprise laboratory system, you can install all CVP components on a single machine and must install all components at the same time. If you are deploying an IPCC Enterprise production system, you can install individual components on different machines. To maximize performance, do not install the Voice Browser or Application Server on the Media Server, to which you copy System Media Files.</td>
</tr>
<tr>
<td>8.</td>
<td>Install CTI Server. Install and configure CallManager Install and configure ICM Install and configure IP IVR or CVP</td>
<td>The CTI Server is an ICM component that allows an external CTI application to communicate with a PG. The CTI Server is part of the Cisco Enterprise CTI product. You can install the CTI Server on the same machine as the Peripheral Gateway software or on a separate machine.</td>
</tr>
<tr>
<td>9.</td>
<td>Install CTI OS software or CAD software, depending on which agent/supervisor desktop software you are deploying. Install CTI Server.</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>Optionally, install the Cisco Collaboration Server software. Install and configure ICM.</td>
<td>Collaboration Server must be installed before ICM can be configured for Multichannel routing.</td>
</tr>
<tr>
<td>11.</td>
<td>If you have installed the Cisco Collaboration Server, optionally install Dynamic Content Adapter. Install and configure Cisco Collaboration Server.</td>
<td>There are no IPCC-specific installation instructions for the Dynamic Content Adapter.</td>
</tr>
</tbody>
</table>
### IPCC Enterprise Component Software Configuration Tasks

This section lists the basic configuration tasks for each IPCC component/functionality area. The component/functionality areas that must be configured specially for IPCC include:

1. CallManager
2. IP IVR (if deployed)
3. ICM
4. Outbound Option
5. CVP (if deployed)
6. Agent And Supervisor Desktops
7. Multichannel applications (if deployed)
8. Reporting

<table>
<thead>
<tr>
<th>Task</th>
<th>IPCC Installation Prerequisites</th>
<th>IPCC Installation Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.</td>
<td>If you have installed the Cisco Collaboration Server, optionally, install Cisco Media Blender.</td>
<td>Install and configure Cisco Collaboration Server.</td>
</tr>
</tbody>
</table>

---

*Cisco Internet Service Node Installation Guide*
*Cisco Customer Response Solutions Getting Started Guide (for IP IVR installation)*
*Cisco Internet Service Node Installation Guide*
*ICM Installation Guide for Cisco ICM Enterprise Edition*
*CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*
*Installation Guide: Cisco Desktop Product Suite*
*Cisco Collaboration Server Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*
*Cisco Media Blender Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*
### CallManager Configuration Tasks

The following table lists the configuration tasks required to CallManager in an IPCC Enterprise deployment. These tasks should be performed in the order listed. For detailed instructions, see Chapter 4, “Installing and Configuring Cisco CallManager for IPCC Enterprise.”

<table>
<thead>
<tr>
<th>CallManager Configuration Tasks</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 Call Manager. The Route Points for dialed numbers must still be created in CallManager Administration.</td>
</tr>
<tr>
<td>3. Configure the CTI Ports</td>
<td>Only necessary for IP IVR deployments.</td>
</tr>
<tr>
<td></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 Call Manager.</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 CallManager PG, and one account to associate with IP IVR and the CTI Ports. Note: If you are using IP IVR 4.0(x) or later, JTAPI users can be configured directly in the IP IVR Administration interface; you do not need to configure them in Call Manager.</td>
</tr>
</tbody>
</table>
IP IVR Configuration Tasks

The following table lists the configuration tasks required to IP IVR in an IPCC Enterprise deployment. These tasks should be performed in the order listed. For detailed instructions, see Chapter 5, “Installing and Configuring Cisco IP IVR for IPCC Enterprise.”

<table>
<thead>
<tr>
<th>IP IVR Configuration Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Configure JTAPI user on the IP IVR.</td>
<td>Use information from CallManager JTAPI users.</td>
<td></td>
</tr>
<tr>
<td>3. Configure CTI Port Groups.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Configure the ICM subsystem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Create and upload VRU scripts.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Configure IP IVR for ICM Translation Routing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Configure and start the Application Engine</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ICM Configuration Tasks

The following table lists the configuration tasks required to ICM in an IPCC Enterprise deployment. These tasks should be performed in the order listed. For detailed instructions, see Chapter 6, “Installing and Configuring Cisco ICM for IPCC Enterprise.”

<table>
<thead>
<tr>
<th>ICM Configuration Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure agent desk settings.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Configure a Network VRU.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Configure and install either the System PG or the Generic PG.</td>
<td>You must configure the PG before installing it. Generally speaking, you would use the: System PG if you are deploying IP IVR. Generic PG if you are deploying CVP.</td>
<td></td>
</tr>
<tr>
<td>4. Install JTAPI Client on the System or Generic PG.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Configure and install the MR PG</td>
<td>You create MR PGs only if you are deploying Outbound Option or the Multichannel options. You must configure the MR PG before installing it.</td>
<td></td>
</tr>
<tr>
<td>6. Configure network trunk groups.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Configure trunk groups.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Configure the Network VRU Bank.</td>
<td>For System PG deployments only.</td>
<td></td>
</tr>
<tr>
<td>9. Configure services.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix A      IPCC Enterprise Checklists and Worksheets

IPCC Enterprise Component Software Configuration Tasks

### Outbound Option Configuration Tasks

The following table lists the Outbound Option configuration tasks required in an IPCC Enterprise system. These tasks should be performed in the order listed. For detailed instructions, see Chapter 7, “Installing and Configuring Outbound Option for IPCC Enterprise.”

<table>
<thead>
<tr>
<th>Outbound Option Configuration Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure ICM for Outbound Option</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Configure CallManager for Outbound Option</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Create routing and administration scripts.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### CVP Configuration Tasks

The following table lists the configuration tasks required to CVP in an IPCC Enterprise deployment. These tasks should be performed in the order listed. For detailed instructions, see Chapter 8, “Installing and Configuring Cisco CVP for IPCC Enterprise.”

<table>
<thead>
<tr>
<th>CVP Configuration Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure the Application Server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Configure the Voice Browser.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Set up Cisco Gateways/Gatekeepers to interact with CVP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Define CVP Voice Browser as a gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Update Cisco Listener and Alarm Tracker software to support SDDSN.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Agent and Supervisor Desktop Configuration Tasks

The following table lists the configuration tasks required for Agent and Supervisor Desktops in an IPCC Enterprise deployment. These tasks should be performed in the order listed. For detailed instructions, see Chapter 9, “Installing Agent and Supervisor Desktops for IPCC Enterprise.”

<table>
<thead>
<tr>
<th>Desktop Installation Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install and configure CTI OS Server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Install CTI OS Agent and Supervisor desktops, OR install CAD Agent and Supervisor Desktops</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Start CTI OS Services</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Multichannel Configuration Tasks

The following table lists the configuration tasks required for Multichannel components in an IPCC Enterprise deployment. These tasks should be performed in the order listed. For detailed instructions, see Chapter 10, “Installing and Configuring Cisco Multichannel Components for IPCC Enterprise.”

<table>
<thead>
<tr>
<th>Multichannel Configuration Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure Media Routing Domains</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Configure Application Instances</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Establish Administration Connections</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Set ECC (Expanded Call Context) Variables</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Write ICM Routing Scripts for Multichannel Options</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Configure Cisco Web Collaboration Server for ICM Integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Configure Cisco Media Blender for ICM Integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Configure Cisco E-Mail Manager for ICM Integration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note

The Dynamic Content Adaptor requires no integration configuration with ICM. Its relationship with ICM is established through its integration with Cisco Collaboration Server. See the Cisco Dynamic Content Adapter Installation and Integration Guide for instruction on integrating the DCA with Cisco Collaboration Server.
IPCC Reporting Configuration Tasks

The following table lists the reporting configuration tasks required in an IPCC Enterprise system. These tasks should be performed in the order listed. For detailed instructions, see Chapter 11, “How to Configure Reporting for IPCC Enterprise.”

<table>
<thead>
<tr>
<th>Reporting Configuration Task</th>
<th>Notes</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure Agent Reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Configure Service Levels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Configure Bucket Levels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Configure IVR Applications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Optionally, modify Short Calls configuration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IPCC Enterprise Configuration Values Worksheets**

This section provides worksheets you can use to plan and record the values you will use to configure IPCC Enterprise. Separate worksheets are provided for production and laboratory environments. The laboratory worksheet is pre populated with the sample lab values used throughout this guide.

**IPCC Enterprise Production Environment Configuration Worksheet**

You can use the table below as a worksheet to record the values you enter on each IPCC Enterprise component during installation and configuration. In the table, grey cells indicate configuration items that do not pertain to a specific component.

If the worksheet does not contain enough rows for you to enter all of your configuration values (for example, you configure 30 agents and the worksheet contains only two rows for agents), you can use the worksheet to indicate a file containing all of the values for that item.

<table>
<thead>
<tr>
<th>Item</th>
<th>CallManager</th>
<th>IP IVR</th>
<th>CVP</th>
<th>ICM</th>
<th>CCS &amp; CEM</th>
<th>CTI OS</th>
<th>CAD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Route Point</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Route Point</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Route Point</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>CallManager</td>
<td>IP IVR</td>
<td>CVP</td>
<td>ICM</td>
<td>CCS &amp; CEM</td>
<td>CTI OS</td>
<td>CAD</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------</td>
<td>--------</td>
<td>-----</td>
<td>-----</td>
<td>-----------</td>
<td>--------</td>
<td>-----</td>
</tr>
<tr>
<td>CTI Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM JTAPI User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP IVR JTAPI User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Port Group number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IVR Flow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IVR Flow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VRU Connection Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM PG Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM PIM Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Controller ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peripheral ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP IVR PIM Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Controller ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peripheral ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTI Server Connection Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network VRU Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP IVR Network Trunk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP IVR Trunk Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP IVR TG Peripheral#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM PG Peripheral Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM PG Peripheral Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM PG Network Trunk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM PG Trunk Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>CallManager</td>
<td>IP IVR</td>
<td>CVP</td>
<td>ICM</td>
<td>CCS &amp; CEM</td>
<td>CTI OS</td>
<td>CAD</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------</td>
<td>--------</td>
<td>-----</td>
<td>-----</td>
<td>-----------</td>
<td>--------</td>
<td>-----</td>
</tr>
<tr>
<td>MR VRU Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MR PG Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collaboration MR PIM Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Controller ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peripheral ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-Mail Manager MR PIM Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Controller ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peripheral ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blended Agent PIM Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Controller ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peripheral ID#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BA Dialer Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BA Dialer Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BA Dialer Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Routing Domains</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ConAPI Connections (registry port)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SVC Virtual Ext.#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skill Group #1 Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skill Group Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG Virtual Ext.#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skill Group #2 Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skill Group Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>CallManager</td>
<td>IP IVR</td>
<td>CVP</td>
<td>ICM</td>
<td>CCS &amp; CEM</td>
<td>CTI OS</td>
<td>CAD</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>--------</td>
<td>-----</td>
<td>-----</td>
<td>-----------</td>
<td>--------</td>
<td>-----</td>
</tr>
<tr>
<td>SG Virtual Ext.#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Setting Up an IPCC Enterprise Laboratory System

This appendix provides advice on how to set up IPCC Enterprise in a laboratory environment. It contains these sections:

- About IPCC Enterprise Laboratory Hardware Requirements, page B-1
- About Installing an ICM Sprawler, page B-2

About IPCC Enterprise Laboratory Hardware Requirements

Using IPCC Enterprise in a laboratory environment requires less equipment than you would need in a production environment. A laboratory that includes Outbound Option and multichannel components can be deployed on as few as six boxes for a laboratory setup. In a more heavily trafficked production environment, you would install IP IVR and the ICM Logger on separate machines. The CTI OS Agent and Supervisor Desktops would also be separated, and Collaboration Server and E-Mail Manager would each require two machines (one for the database server and one for the client).

The following minimum hardware is required in an IPCC Enterprise laboratory. See the Cisco ICM/IPCC Enterprise 7.0(0) Bill of Materials for box specifications and OS requirements.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IP phones</td>
<td>Model 7960 (three or more)</td>
</tr>
<tr>
<td>Cisco CallManager + IP IVR server</td>
<td>1 Cisco Media Convergence Server (MCS) or equivalent</td>
</tr>
<tr>
<td>ICM (router, logger, AW, PG) + CTI Server + CTI OS Server +</td>
<td>1 Cisco Media Convergence Server (MCS) or equivalent</td>
</tr>
<tr>
<td>Outbound Option Dialer (optional) + CTI OS Agent and Supervisor</td>
<td></td>
</tr>
<tr>
<td>Desktops or CAD Agent/Supervisor Desktop server</td>
<td></td>
</tr>
<tr>
<td>Cisco Media Blender server (optional)</td>
<td>1 Cisco Media Convergence Server (MCS) or equivalent</td>
</tr>
<tr>
<td>Cisco Collaboration Server server (optional)</td>
<td>1 Cisco Media Convergence Server (MCS) or equivalent</td>
</tr>
</tbody>
</table>

**Note:** CCS can also run on Sun Sparc workstations running Solaris 8. See the Cisco Collaboration Server Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions for more information.
About Installing an ICM Sprawler

For a laboratory setup, you can choose to install all of the ICM software components on one server, called a sprawler.

**Note** You can also choose to install the ICM software on more than one machine, and you need more than one machine in a production environment. See the Alternative Lab Setup system diagram for an example of the ICM components installed on two machines.

Before configuring the ICM software in the laboratory, ensure that the Windows 2000 planning and pre-installation tasks are complete.

## How to Install ICM Components on a Sprawler

In a production environment, you typically install ICM components on several different machines. In a laboratory environment, however, you can install all ICM software components on a single machine, called a *sprawler*. You can install the following ICM components on a sprawler:

- Admin Workstation
- Logger
- Router
- PGs
- CTI Server

### Cisco Dynamic Content Adapter server (optional)

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Dynamic Content Adapter server (optional)</td>
<td>1 Cisco Media Convergence Server (MCS) or equivalent</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The DCA can also run on Sun Sparc workstations running Solaris 8. See the Dynamic Content Adapter Installation and Integration Guide for Cisco ICM/IPCC Enterprise &amp; Hosted Editions for more information.</td>
</tr>
</tbody>
</table>

| Cisco E-Mail Manager server (optional) | 1 Cisco Media Convergence Server (MCS) or equivalent |
A sprawler installation requires some specific installation settings for each ICM component. These are listed in the table below.

<table>
<thead>
<tr>
<th>When Installing the:</th>
<th>Do the Following:</th>
</tr>
</thead>
</table>
| Admin Workstation    | 1. On the Admin Workstation Properties dialog box, select the Real-time Distributor button.  
                              2. On the Real-time Distributor Node Properties dialog box, select the Web-based Monitoring check box, clear the Router and Logger Side B fields, and select Historical Data Server.  
                              3. Under Node Manager Properties, enable the CMS node check box.  
                              4. When using the ICM Database Administrator tool to create a Historical Data Server database, set the data size to 500 MB and the Log size to 100 MB. |
| CallRouter           | 1. On the Router Properties dialog box, select Production Mode, No system reboot on error, and Side A.  
                              2. On the Router Component Properties dialog box, leave the Network Interface Controllers unchecked.  
                              4. On the Network Interface Database dialog box, clear all Node B fields. |
| Logger               | 1. On the Logger Properties dialog box, in addition to the defaults, select Historical Data Replication.  
                              2. On the Logger Component Properties dialog box, make sure nothing is selected unless you are using Outbound Option. The Outbound Option Campaign Manager resides on the Logger. Note that you can install one Outbound Option Dialer and Campaign Manager on the ICM sprawler.  
                              3. On the Network Interface Properties dialog box, clear all Node B fields.  
                              4. When using the ICM Database Administrator tool to create a Historical Data Server database, set the data size to 500 MB and the Log size to 100 MB.  
                              5. When using the ICM Database Administrator tool to create the Outbound Option private database, set the data size to 300 MB and the Log size to 100 MB. |
### About Installing an ICM Sprawler

The following system diagram shows another possible setup of the IPCC Enterprise laboratory system, one that does not install the ICM software as a sprawler. The ICM software is installed on two machines instead of one and the Cisco Media Blender is installed on the machine with the peripheral gateways.

<table>
<thead>
<tr>
<th>When Installing the:</th>
<th>Do the Following:</th>
</tr>
</thead>
</table>
| **Generic or System PG** | 1. On the Peripheral Gateway Network Interfaces dialog box, make note of the logical controller ID and select the Service Control and Queue Reporting options.  
  3. On the Peripheral Gateway Network Interfaces dialog box, remove any value references for Side B. |
| **CTI Server** | 1. On the CTI Server Properties dialog box, choose Production mode and Side A. In the CG node properties section of that box, select a CG Node from the ID field drop-down list. Be sure that the CG number matches the PG number; for example, for PG1, the ID field should read CG1.  
  2. On the CTI Server Component Properties dialog box, make a note of the Client Connection Port Number, which is typically 42027.  
  3. On the CTI Network Interface Properties dialog box, be sure that there are values for Node A but none for Node B in the three sections of that box. |

### An Alternative Setup to a Sprawler

The following system diagram shows another possible setup of the IPCC Enterprise laboratory system, one that does not install the ICM software as a sprawler. The ICM software is installed on two machines instead of one and the Cisco Media Blender is installed on the machine with the peripheral gateways.
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 Solution Reference Network Design Guide.

How to Configure CallManager for Fault Tolerance

This section describes methods of configuring CallManager to improve fault tolerance in your IPCC system. These include:

- How to Set Up a Recovery Number for Your IPCC System, page C-1
- How to Improve Failure Detection, page C-1

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, you should configure Call Forward No Answer and Call Forward Busy on the CTI Route Points for the CallManager PG and the IP IVR to point to this recovery number.

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

How to Improve Failure Detection

The CallManager PG 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; we recommend changing this to the minimum value of 5.

To change the heartbeat interval:

1. From the Start menu, select Programs -> Cisco JTAPI -> JTAPI Preferences.
2. Set the Advanced -> Server Heartbeat Interval (sec) field to 5 seconds.
## Symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ASSUME_ANSWERED</td>
<td>11-5</td>
</tr>
</tbody>
</table>

## A

### Abandoned short calls
- configuring | 11-6

### Agents
- enabling reporting | 11-2

### Answered short calls
- configuring | 11-7

### Application connections | 10-8

## B

### Barge-in | 11-7

## C

### Call type service levels | 11-4, 11-5

### Call variable
- VruStatus | 6-42

### CMS Server, configuring connections | 10-9

### Configuring
- CMS Server connections | 10-9

## D

### dynamic routing client | 8-8

## E

### ECC variables
- for integrated applications | 10-10

### Emergency assist | 11-7

### Enterprise service levels | 11-3, 11-4, 11-5

## I

### Intercept | 11-7

### IVR applications
- call flow through | 11-5

## J

### JTAPI Client
- Update Tool | 5-12

## N

### Nodes, Queue to Agent | 10-7

## P

### Physical interface controllers | 6-13, 6-18

## Q

### Queue to Agent node | 10-7

## R

### Reporting
Index

service levels 11-3, 11-4
short calls 11-6

S

Service Control interface 5-8
Service levels 11-3, 11-4
at the call type 11-4, 11-5
at the enterprise 11-3, 11-4, 11-5
Short calls 11-6
configuring abandoned 11-6
configuring answered 11-7
Supervisor assist 11-7
Supervisory features 11-3
  barge-in 11-7
  intercept 11-7

T

Translation routes
  deleting 6-40
  reports 6-40
  updating 6-40
Translation Route to VRU 8-9

V

VRU Error Checking 6-42