ICM Installation Guide for Cisco ICM Enterprise Edition

Release 7.0(0)

July 2005

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-1400

Table of Contents

Preface

Purpose

This manual describes how to install the components of the Cisco Intelligent Contact Management software. It includes information about hardware configuration and software setup.

Audience

This document is intended for anyone installing one or more components of the Intelligent Contact Management software.

Organization

The following table describes the information contained in each chapter of this guide.

Chapter	Description
Chapter 1, "Introduction"	Includes references to Pre-Installation documentation. Describes how to get started with the ICM Setup program.
Chapter 2, "CallRouter Setup"	Explains how to install and configure the CallRouter software.
Chapter 3, "Logger Setup"	Explains how to install and configure the Logger software.
Chapter 4, "Admin Workstation Setup"	Explains how to install and configure the Admin Workstation software.
Chapter 5, "Network Interface Controller Setup"	Explains how to configure devices for Network Interface Controllers.
Chapter 6, "Peripheral Gateway Setup"	Explains how to install and configure the Peripheral Gateway software.
Chapter 7, "CTI Server Setup"	Explains how to install and configure the CTI Gateway software.

Chapter	Description
Chapter 8, "After the Installation"	Provides post-installation information, in particular, information on what the ICM Setup program installs, including directories and their contents, and Windows services.

Related Documentation

For additional information about Cisco Intelligent Contact Management (ICM) software, see the **Cisco web site** (http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm) listing ICM documentation.

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

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

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD from the Ordering tool or Cisco Marketplace.

Cisco Ordering Tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL::

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

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Instructions for ordering documentation using the Ordering tool are at this URL:

  http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

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

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

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

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL: **http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html**

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL: **http://www.cisco.com/go/psirt**

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL: **http://www.cisco.com/en/US/products/products_psirt_rss_feed.html**

Reporting Security Problems in Cisco Products

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

- Emergencies - 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.

- Nonemergencies - psirt@cisco.com

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

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

Note: We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x. Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list: **http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on**

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

http://tools.cisco.com/RPF/register/register.do

Note: Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

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

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

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or

severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

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

  http://www.cisco.com/en/US/learning/index.html

Chapter 1

Introduction

This manual explains how to install the major components of Intelligent Contact Management (ICM) software. The ICM platform is a contact routing system that runs on several PCs (or *nodes*) which may be distributed across many sites.

This chapter includes the following:

- Where to find information relating to ICM pre-installation tasks.
- Information you will need before you install ICM components.
- Where to find information about hardware and third-party software requirements for individual ICM components.
- An introduction to the ICM Setup program.

Subsequent chapters explain how to install and configure specific ICM components.

This section contains the following topics:

Pre-Installation Planning

The Cisco Intelligent Contact Management (ICM) software is a distributed software application that routes toll-free calls, web inquiries, and e-mail across geographically distributed contact centers. A typical ICM system includes a number of computers located at different sites.

Because the ICM software works with different types of contact center equipment and sometimes one or more carrier networks, some pre-installation planning is necessary to ensure successful installation of the ICM software.

The pre-installation documentation includes information on topics such as provisioning IXC access, preparing ACDs, and determining the ICM datacom requirements.

For details on ICM software pre-installation planning refer to the *Pre-Installation Planning Guide for Cisco ICM Enterprise Edition*.

Windows Planning and Staging

Understanding and planning for a supported Windows model is a critical task during the planning phase of an ICM software deployment.

During this phase, you must document the specifications of the ICM system and then you must accept them prior to the start of staging a new system. This System Design Specification must include a detailed description and diagrams of the Windows Model for Active Directory and DNS implementation.

For more information on Windows pre-installation requirements, refer to the *Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* and the *SNMP Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

The ICM Components

The principal ICM components are:

- **CallRouter.** The component of the Central Controller that makes routing decisions and both gathers and distributes data from remote sites; generally referred to in this document simply as the Router. (Central Controller is the term used when discussing a CallRouter/Logger configuration.)
- **Logger.** The component of the Central Controller that controls the central database.
- **Admin Workstation.** The human interface to ICM software. An Admin Workstation (AW) can be located at any central or remote site. It allows users to monitor call handling within the system and make changes to configuration data or routing scripts.
- **Network Interface Controller.** The NIC is the interface between the ICM platform and the Interexchange Carrier signaling network.
- **Peripheral Gateway.** The interface between the ICM platform and third-party hardware in each contact center, such as an ACD. A Peripheral Gateway (PG) is typically located at the contact center.
- **CTI Server.** The (optional) component that allows an external CTI application to communicate with a Peripheral Gateway.
- **WebView.** The (optional) component that provides web-based contact center reporting.

The ICM Software CD contains the software for all of these components. You can install any component from the ICM Setup program.

Duplexed Components

To allow ICM software to continue operating when a single node fails, all major components of the system can be duplicated on separate nodes, or duplexed. This allows the system to be fault-tolerant; that is, to continue operating when a component fails.

For example, two computers can run the CallRouter software. If one of those computers fails for any reason, the other computer continues to run and ICM software continues to operate without interruption. The CallRouter and Logger processes are typically duplexed and Peripheral Gateways may be duplexed.

The failure of a single Admin Workstation does not prevent the rest of the ICM system from operating. Therefore, Admin Workstations are not duplexed.

In a fully duplexed configuration, one CallRouter and one Logger compose one side of the Central Controller; the other CallRouter and Logger compose the other side. The sides are called Side A and Side B.

The components of a single side must be located at a single site; that is, the CallRouter and Logger for Side A must be collocated. For maximum fault-tolerance, the Side B components may be at a different site than Side A.

If a Peripheral Gateway (PG) is duplexed, both PGs (A and B) are typically located at a single site; usually, the same site that contains the contact center equipment. If a disaster causes the entire site to fail, the contact center equipment itself is unavailable. Therefore, having a duplexed PG at another site would provide little benefit.

For more information about the ICM system's fault-tolerant architecture, see the *ICM Administration Guide for Cisco ICM Enterprise Edition*.

Communication Between Components

The ICM platform requires both local and wide area networks for communication among the nodes. Each site requires Ethernet unshielded twisted pair (UTP) for local communications. The ICM uses TCP/IP for communication between sites.

The ICM uses visible networks, which might also be used by other equipment, and private networks that are reserved for its own use.

For information about setting up the networks for the ICM, see the *Pre-Installation Planning Guide for Cisco ICM Enterprise Edition*.

Instances, Customers and Components

An *instance* is a single logical ICM. An instance typically consists of several software components (CallRouter, Logger, Peripheral Gateways, Admin Workstations)—some of which may be duplexed—typically installed on several different computers. A single computer may run multiple components of a single instance or components of multiple instances.

Note: You can also install multiple instances on a single computer. However, ICM has a limitation of 25 instances per machine.

A *customer* is an organization that uses the ICM to manage its contact center enterprise. Each customer has its own dialed numbers, labels, call types, scripts, and scheduled targets. However, all Peripheral Gateways, peripherals, services, skill groups, and so forth are associated with the instance rather than a specific customer. Therefore, customers who share an instance cannot have their own Peripheral Gateways. Such customers, however, can be assigned a network VRU with customer-specific scripts for special call treatment.

The following table summarizes what data can be associated with a specific customer and what data are shared by an entire instance.

.

Table 2: Customer Data and Instance Data

Customer	Instance
Dialed numbers, labels, call types, scripts, scheduled targets, and network VRU scripts.	NICs and PGs; peripherals, trunk groups, peripheral targets, skill targets; regions; announcements; application gateways.

Note: No special security is applied at the customer level. Any Admin Workstation user with access to an instance can choose to view data for any or all customers in that instance. However, you can set up WebView or Quick Edit users who have access to only the data for a specific customer.

Customer Types

You can use the customer concept to support multiple independent organizations with a single ICM instance rather than assigning a separate instance to each organization. However, customers that share an instance have more limited capabilities than a customer using a full instance. The following table summarizes the abilities of these two customer types.

Table 3: Customer Types

Full Instance Customer	Shared Instance Customer
Monitored targets (skill groups, agents, and services) and scheduled targets	Scheduled targets only
Full routing capabilities based on Longest Available Agent, Minimum Expected Delay, and so forth	Percent allocation routing and scheduled targets routing only
Dedicated Peripheral Gateways	No dedicated Peripheral Gateways
Admin Workstation, Quick Edit, and/or WebView access	Quick Edit or WebView access only
Full configuration, scripting, and administration capabilities	Limited script modifications through Advanced Services Terminal

Note that all configuration and scripting for a shared instance customer must be performed by the service provider that manages the instance. The customers themselves can only perform Quick Edits within a script.

Before You Install an ICM Component

Before you install ICM software, the computers must have the Microsoft Windows operating system—including SNMP and (for Windows 2003) WMI—and, for some components, Microsoft SQL Server database management software installed.

Additionally, you must have set up the Windows Active Directory services for ICM software. You must have added the Cisco Root Organizational Unit, and at least one Facility Organizational Unit with one Instance Organizational Unit.

Refer to the *Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* and the *SNMP Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

You must **not** install ICM components on a Domain Controller or on a DNS server.

If you are installing WebView, there are third-party components that you must first install on the machine where you are installing WebView. Refer to the *WebView Installation and Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for further information.

You must also ensure that you have enough disk space available on each computer to install the ICM component or components.

If localization is of concern to you, note that English ICM components can be installed on supported localized Windows operating systems, as specified in the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials*. Localized ICM components can be installed only on Windows operating systems localized in the same language.

Hardware and Third-Party Software Compatibility List

Windows Setup automatically checks your hardware and software and reports any potential conflicts. To ensure a successful installation, however, check to make sure your computer hardware is compatible with Windows Server before starting Setup.

To do this, check the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials* (BOM). If your hardware is not listed, Setup might not be successful. This document is found at:

http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom

In addition, check that you have updated drivers for your hardware devices and that you have the latest system BIOS. The device manufacturers can assist you in obtaining these items. Finally, before installing Windows Server, consider taking a device inventory of the hardware devices on your computers.

For other hardware information, see

http://www.cisco.com/warp/partner/icsg/service/hw_sw_platform.html

SQL Server

ICM software requires Microsoft SQL Server databases on each Logger, Historical Data Server (HDS), and each Real-time Distributor Admin Workstation (SQL Server is not required for Client AWs). SQL Server must be installed on each of these computers before you install the ICM software.

Refer to the *Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for more information about installing SQL Server software.

Windows Monitoring Tools

SNMP and (for Windows 2003) WMI must be installed. Refer to the *Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* and the *SNMP Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

Machine Names

Cisco has defined a set of conventions for naming ICM computers. The general syntax is as follows:

CSO*SSSCCCM*

The terms in this syntax are as follows:

- *SSS* is a unique short code (maximum five letters) that identifies the entire system.
- *CCC* is a two- or three-letter code indicating the component type.
- *M* is a one- or two-character machine identifier (typically, the side and/or a device number).

Your ICM support provider will supply you with a unique system identifier. The following table lists the codes and machine identifiers for each component type.

Table 4: Component Codes

Component Type	Code	Machine IDs
Admin Workstation	AW	1, 2, 3, . . .
CallRouter	RTR	A or B
CTI Server	CG	1A, 1B, 2A, 2B, 3A, . . .
Logger	LGR	A or B
Network Interface Controller	NIC	1A, 1B, 1C, 1D, . . .; 2A, 2B, 2C, 2D, . . .
Peripheral Gateway	PG	1A, 1B, 2A, 2B, 3A, . . .

For example, if the system identifier is XYZ, the Logger on the B side is named CSOXYZLGRB.

The letter in the NIC's machine code indicates the relative location of the NIC. The first NIC is named 1A. If its duplexed peer is located at the same site, that NIC is named 1B; if the

duplexed peer is located at another site, that NIC is named 1C. If each of two sites contain duplexed NICs, the two at one site are named 1A and 1B and the two at the other site are named 1C and 1D.

Security Considerations

A discussion of security and ICM software can be found in the *Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*, which you have presumably already used in association with the *Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* while installing your Microsoft Windows software and setting up your Windows Active Directory services for ICM software. However, a few specific security topics are mentioned in the following sections.

Cisco Security Agent (CSA)

A standalone Cisco Security Agent (CSA) for ICM software is available as a part of ICM/IPCC 7.0(0). The standalone Cisco Security Agent provides intrusion detection and prevention for Cisco ICM software. Cisco Security Agent removes potential known and unknown ("Day Zero") security risks that threaten enterprise networks and applications. It dramatically reduces downtime, widespread attack propagation and clean-up costs. The Agent is provided free of charge by Cisco Systems for use with release 7.0(0) of the Cisco ICM software. While Cisco highly recommends its installation, it is optional. For more information refer to the *Cisco Security Agent Installation/Deployment Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

Some considerations to keep in mind are the following:

- If you plan to use Cisco Security Agent, you must always use the default directories when installing any software on a server. You need not choose the default disk drive if an option is available (for example, C: or D:), but you must use default directories.
- You must disable the Cisco Security Agent service before performing any software installation. This includes not only Cisco ICM software, but also third-party software that you intend to use with the ICM software. Ensure that the service does not get enabled at any time during the installation or upgrade. Failure to do so may cause problems with the installation or upgrade. After installing or upgrading the software, you must reenable the Cisco Security Agent service. With the service disabled, the Agent no long provides intrusion detection for the server.

Note: The actions described in the last bullet do not have to be done manually, since ICM Setup will offer to disable and reenable CSA for you.

Secure Socket Layer (SSL)

By default, Secure Socket Layer (SSL) authentication is enabled on Windows 2003 systems for the web applications: WebView (refer to the *WebView Installation and Administration Guide*

for Cisco ICM/IPCC Enterprise & Hosted Editions for more information), Agent Re-skilling Web Tool, and Internet Script Editor—if any or all of these optional applications are selected.

An SSL Encryption Utility, sslutil.exe, is also provided in \icm\bin if you wish to change the default settings.

Security Hardening Checkbox

A **Prompt for Security Hardening checkbox** is provided as part of Setup. If the box is checked, each time that Setup is run, you are prompted to apply security hardening—if security hardening has not been applied, or if an updated template is available. This option is available only on Windows 2003 systems.

See Also

For the Prompt for Security Hardening checkbox in Setup, Cisco ICM Setup Dialog Box (page 19).

Windows Firewall Service

If you wish to install Windows Firewall service in a manner consistent with ICM software, use the following procedure:

1. Install Cisco ICM Release 7.0
2. Deploy the CiscoICMFirewallConfig script (see "Windows Firewall Configuration" in Chapter 8)
3. Start ICM services

Note: Any subsequent installation of a new component will require re-deploying the Windows Firewall Configuration script.

For more information, refer to the *Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

See Also

Windows Firewall Configuration (page 103).

Setup Warning Messages

ICM displays a warning message for the following conditions:

- **CSA Installed**. A message may display when you have the Cisco Security Agent installed on your system and you are running the Setup program. If the current version of CSA (CSA

4.5) is running, Setup displays a warning message and asks for permission to stop CSA. If permission is granted, Setup stops CSA, and when installation is completed, automatically restarts CSA. If you have CSA installed but it is not the current version, a message displays (whether or not CSA is running) telling you that you do not have the latest version.

- **ICM patches applied**. This warning displays when you click the Upgrade All button, if Setup detects that Service Releases and/or Engineering Specials have been installed on the machine. You must uninstall any Services Releases and Engineering Specials and rerun the Setup program.
- **SNMP not installed**. This warning is displayed by Setup if SNMP is not installed.
- **WMI not installed** (on Windows 2003). This warning is displayed by Setup on a Windows 2003 operating system if WMI is not installed.

Installing RMS Update Files

The ICM CD contains a separate installer program that allows you to update the RMS files for Listener and AlarmTracker.

To install the RMS update files:

Step 1 From the ICM CD, open the RMSEventFileUpdate folder.

Step 2 Double-click on Setup.exe. The RMS Event File Update screen displays.

Step 3 Click **Next** to install the update.

Step 4 Click **Finish** when the update is complete.

About Beginning Installation

Note: In order to run Setup, you must be a local administrator and belong to the setup group for any instance for which you are installing a component.

You can install the various components in the order in which they are treated in this manual. In general, there is a great deal of flexibility in the order of installation provided that you know

the names and locations for the various components beforehand. However, the following presents the usual approach:

- Install either the CallRouter or the Logger first. It does not matter in which order you install the CallRouter and Logger.
- Install both the CallRouter and the Logger before you install an Admin Workstation (AW).
- If you are using WebView, install it after you have installed the Real-time Distributor AW.
- Install the CallRouter, Logger, and AW before you install the Network Interface Controller (NIC) and Peripheral Gateway (PG), but it does not matter in which order you install the NIC and PG.
- Install the CTI Server after you have installed the CallRouter, Logger, AW, NIC, and PG.

How to Begin the Installation Process

You begin the installation process for any ICM software component by running the Setup program from the ICM Software CD.

Note: Beginning with ICM 7.0(0), various installations can be performed using the local version of ICMSetup in \icm\bin, as well as the Setup on the CD—see Post-Installation Setup.

Step 1 Mount the ICM Software CD.

Step 2 Find and run the file Setup.exe at the top level of the CD. The Cisco ICM Setup dialog box opens.

See Also

For the two versions of Setup, Post-Installation Setup (page 20).

Cisco ICM Setup Dialog Box

The Cisco ICM Setup dialog box allows you to add, edit, and delete Instances and, for each instance, Components. It also includes:

1. **Domain Manager button**—clicking on this button initiates an executable program, independent from Setup, that can be run at any time to create or remove any of the Active Directory Organizational Units (OUs), or to add or remove user login accounts to security

groups for each of the OUs; refer to the *Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

2. **Upgrade All button**—use this button when upgrading a system to a newer version of ICM; refer to the *ICM Upgrade Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

3. **Prompt for Security Hardening checkbox**—checking this box causes Setup, each time it is run, to prompt the user to apply security hardening (if security hardening has not been applied, or if an updated template is available). This option is available only on Windows 2003 systems.

See Also

For adding, editing, and deleting instances, How to Add an Instance (page 21), and the following sections. For installing a component, How to Install a Component (page 23).

Post-Installation Setup

A local version of the Setup program is installed as part of each ICM component, namely, \icm\bin\ICMSetup.exe. (On an Admin Workstation, the Cisco Admin Workstation group contains an icon for this program.) Prior to ICM 7.0(0), this local version only allowed you to change the configuration settings of the software after it was installed. It did not allow you to install new software—to install or reinstall software, you had to run Setup from the CD.

For ICM 7.0(0), the following table indicates what occurs when certain actions are performed using Setup from the CD, or using ICMSetup in \icm\bin—both when patches (Service Releases and/or Engineering Specials) have been applied and when patches have not been applied.

Action	Patches	CD Setup	\icm\bin\ICMSetup
Add Instance	Yes/No	Instance is added.	Instance is added.
Edit Instance	Yes/No	Domain, Facility and/or Instance Number can be changed. The modification has to be completed by running Upgrade All or editing each component.	Instance Number can be changed. The modification has to be completed by editing each component.
Delete Instance	Yes/No	Instance is deleted. (Instance specific folders, registries, services and AT jobs are deleted; files in \icm\bin are not affected.)	Instance is deleted. (Instance specific folders, registries, services and AT jobs are deleted; files in \icm\bin are not affected.)
Upgrade All	Yes	Setup displays an error message, asking that patches be removed.	Not Applicable (Upgrade All button is disabled)
Upgrade All	No	Setup upgrades files, overwriting files in \icm\bin.	Not Applicable (Upgrade All button is disabled)

Action	Patches	CD Setup	\icm\bin\ICMSetup
Add Component	Yes	If a new component is being added (for example, you are setting up your first Logger), Setup displays an error message, asking that patches be removed. If an already existing component is being added (for example, you are setting up your second Logger), the component is added.	If an already existing component is being added (for example, you are setting up your second Logger), the component is added. New components (for example, you are setting up your first Logger) cannot be added.
Add Component	No	Component is added.	If an already existing component is being added (for example, you are setting up your second Logger), the component is added. New components (for example, you are setting up your first Logger) cannot be added.
Edit Component	Yes	Component is edited, but the files in \icm\bin are not overwritten.	Component is edited, but the files in \icm\bin are not overwritten.
Edit Component	No	Component is edited, and the files in \icm\bin are overwritten.	Component is edited, but the files in \icm\bin are not overwritten.
Delete Component	Yes/No	Component is deleted. (Component specific folders, registries, services and AT jobs are deleted; files in \icm\bin are not affected.)	Component is deleted. (Component specific folders, registries, services and AT jobs are deleted; files in \icm\bin are not affected.)

Installing Multiple Components

In some cases, you might want to install more than one ICM component on a single computer. For example, you might install the CallRouter and Logger software on a single node. In this case, you must run Setup for each component. Similarly, to install a specific component for more than one customer, you must run Setup for each instance.

How to Add an Instance

You must add at least one ICM instance before you can install any ICM components.

Note: Before you can create an ICM instance, you **must** have set up the Windows Active Directory services for ICM software. You must have added the Cisco Root Organizational Unit, and at least one Facility Organizational Unit with one Instance Organizational Unit. Refer to the *Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

Step 1 In the Cisco ICM Setup dialog box, in the **ICM Instances** section, click **Add**. The Add Instance dialog box opens.

Step 2 Select the network **Domain** for the instance.

Step 3 Select the **Facility** Organizational Unit for the instance.

Step 4 Select the **Instance Name** for the instance.

Note: The ICM Instance Name is the name of the Instance Organizational Unit.

Step 5 Use the **Instance Number** generated by the ICM software. (For standard single-instance ICM configurations, the instance number is 0.)

Note: The mappings of instance names to instance numbers must be the same on every node in the system.

Step 6 Click **OK**.

See Also

Cisco ICM Setup dialog box (page 19).

How to Edit an Instance

When editing an instance, you can only change the Domain, the containing Facility Organizational Unit, and/or the Instance Number.

Note: The modification has to be completed by running Upgrade All or editing each component.

Step 1 In the Cisco ICM Setup dialog box, in the **ICM Instances** section, select the instance to edit and click **Edit**. The Edit Instance dialog box opens.

Step 2 Optionally, change the Domain, Facility Organizational Unit, and/or Instance Number.

Step 3 Click **OK**.

See Also

Cisco ICM Setup dialog box (page 19).

How to Delete an Instance

Only delete an ICM instance when you are sure it is no longer needed.

Note: It is not necessary to delete ICM components that are part of an instance before deleting the instance; deleting the instance will delete these components.

Step 1 In the Cisco ICM Setup dialog box, in the **ICM Instances** section, select the instance to delete and click **Delete**. The Delete Instance dialog box opens.

By default, the following items are selected to be deleted for the instance:

- Registry Entries
- Files and Directories
- Services
- Security Settings

Step 2 Optionally, change the selections in the Delete Instance dialog box.

Step 3 Click **OK**.

See Also

Cisco ICM Setup dialog box (page 19).

How to Install a Component

Step 1 In the Cisco ICM Setup dialog box, in the **ICM Instances** section, select an ICM Instance.

Step 2 In the **Instance Components** section, click **Add**. The ICM Component Selection dialog box opens.

Step 3 Click on the component that you want to install.

Step 4 After you select a component, Setup leads you through a series of dialog boxes in which you specify configuration settings.

After you have set the configuration values, Setup copies the files to your local disk and performs some initialization and customization procedures. During this time, Setup indicates its progress.

If Setup detects that less than 5% of the space on a disk is available, the Low indicator turns red. (This indicates low space on one of the drives to which files are being copied: either the drive you chose for the installation or the drive where the Windows OS is installed.) If this happens, you can create space by deleting unnecessary files or moving files to another disk. Setup does not reset the Low indicator or the disk space bar until it has finished copying and configuring the files.

In some cases, Setup cannot copy one or more files because it would have to overwrite a file that is in use. If this happens, Setup installs all the files it can and then prompts you to restart the computer.

Save any work in progress in other programs before choosing to restart the computer. When the computer shuts down, Setup is able to overwrite the files. When the computer restarts, the installation is complete.

Step 5 If Setup successfully copies all the files, it displays the final screen and asks whether you want to start the ICM Node Manager.

Step 6 Click **Finish** to complete the component setup and optionally start the Node Manager. If you choose to start it, the Node Manager automatically starts the other ICM processes for the component you installed. Regardless of your choice, the main Setup screen reappears so that you can install another component.

See Also

Cisco ICM Setup dialog box (page 19); Component Selection dialog box (page 24).

ICM Component Selection Dialog Box

In the ICM Component Selection dialog box are the following buttons, used to install the corresponding components:

- **Admin Workstation**—see How to Install an Admin Workstation (page 43)
- **Router**—see How to Install a CallRouter (page 25)
- **Logger**—see How to Install a Logger (page 34)
- **Network Gateway**—ICM Network Gateway software is installed on a dedicated Windows machine that provides SS7 protocol handling; refer to the *Pre-Installation Planning Guide for Cisco ICM Enterprise Edition*, and see the online help
- **MEI Server**—refer to the *Cisco ICM Software ACD Supplement for Nortel Meridian*
- **WebView**—refer to the *WebView Installation and Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*
- **Peripheral Gateway**—see How to Install a Peripheral Gateway (page 61)
- **CTI Server**—see How to Install CTI Server (page 95)
- **Application Bridge Server**—see How to Install an Aspect Application Bridge Server (page 86)
- **CompuCALL Server Gateway**—see How to Install a DMS-100 CompuCALL Server Gateway (page 88)
- **Outbound Option Dialer**—refer to the *Outbound Option Setup and Configuration Guide for Cisco ICM/IPCC Enterprise & IPCC Hosted Editions*

Chapter 2

CallRouter Setup

Before You Install CallRouter

The CallRouter (generally referred to in this document simply as the Router) is the component that contains the contact routing logic and makes all routing decisions. It receives contact routing requests and determines the best destination for each contact. It also collects information about the entire system.

Before you install the CallRouter software, the Windows operating system (for version specifics refer to the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials*)—including SNMP and (for Windows 2003) WMI—must be installed on the computer, you must have set up the Windows Active Directory services for ICM software, and you must have set up at least one ICM instance.

This chapter explains how to install the CallRouter software and perform some basic configuration. For this configuration, you must know the visible and private network addresses (either host names or IP addresses) of the CallRouter and, for a duplexed configuration, the addresses of the CallRouter on the other Side.

The CallRouter and Logger are typically on separate computers. However, in small contact center configurations they can both be on the same computer.

See Also

Before You Install an ICM Component (page 13); How to Add an Instance (page 21).

How to Install a CallRouter

How to Add a Router Component

Step 1 In the Cisco ICM Setup dialog box, in the left column under ICM Instances, select an instance.

Step 2 Click **Add** in the Instance Components section.

The ICM Component Selection dialog box opens.

Step 3 Click **Router**.

The Router Properties dialog box opens.

See Also

Cisco ICM Setup dialog box (page 19); ICM Component Selection dialog box (page 24).

How to Set Router Properties

Step 1 In the Router Properties dialog box, check **Production mode** and **Auto start at system startup** unless you are specifically told otherwise by your ICM support provider. This ensures that the CallRouter can restart itself automatically if necessary.

Note: However, set the Auto Start feature only **after** your ICM installation is otherwise complete. The server may need to be rebooted a number of times during installation, and problems could occur if the node starts before patches and/or databases are applied.

Step 2 Check the **Duplexed Router** option if you are configuring redundant CallRouter machines.

Step 3 Check the **Database routing** option if you plan to use the ICM's optional database routing feature to route calls based on data read from an external database. This requires that you purchase the DbLink product. You might use this, for example, to look up the caller's telephone number (calling line ID) in your corporate database.

Step 4 Check the **Application gateway** option if you plan to use the ICM's optional custom ICM Application Gateway feature to access an external application from within a routing script. This requires that you purchase the Cisco ICM Application Gateway product.

Step 5 Check the **Remote Network Routing** option if you are installing CallRouter on a NAM—refer to the *Setup and Configuration Guide for Cisco ICM Hosted Edition* regarding this, and other particularities, when installing CallRouter on a NAM.

Step 6 Do not check the **No system reboot on error** option if the machine runs only a single CallRouter component and no other critical applications. This will allow the ICM to reboot the machine when necessary to recover from errors or when the CallRouter specifically requests a reboot.

If multiple instances of the CallRouter run on the same physical machine or if other critical processes run on the machine, check this option. If you choose this option, you may need to manually recover from some failures.

Step 7 If the CallRouter will be duplexed, specify which **Side** you are installing: Side A or Side B. If the CallRouter will be simplexed, choose Side A.

Step 8 Choose the local **Drive** on which you want to install the software.

Note: Be sure to note the drive you are using for future reference, since this information is required when applying software patches.

Step 9 Choose the **Language** from the list.

Step 10 Click **Next**.

Setup loads any current installation settings and then the Router Component Properties dialog box opens.

How to Set Router Component Properties

Note: If you are installing CallRouter on a NAM or CICM, refer to the *Setup and Configuration Guide for Cisco ICM Hosted Edition* for specific information relevant to the Router Component Properties dialog box.

Step 1 In the Router Component Properties dialog box, if you are routing calls with an interface to an IntereXchange Carrier (IXC), or you are using the INCRP or INAP protocols, you must set up the appropriate Network Interface Controller (NIC) within the CallRouter. However, before you can set up a NIC, you must create the related database records using ICM Configuration Manager on an Admin Workstation. If you are performing the initial installation of the ICM, leave the NIC configuration for later.

For information about setting up a NIC, see Chapter 5, "Network Interface Controller Setup".

Step 2 In the **Customer ID** field, enter your unique customer identifier. If you do not know your identifier, check with your ICM support provider.

Step 3 Accept the default values for the **MDS timed delivery queue** unless told otherwise by your ICM support provider.

A partial exception to this last statement is the **Disable ICM time synchronization** box, which is used to select time synchronization service. The box is checked, by default, since the Windows operating system uses its own integrated time service. However, if the machine is a workgroup machine, uncheck this box to enable ICM Time Synchronization. (Note that Setup does not change the current configuration when performing an Upgrade All.)

Step 4 Click **Next**.

The Device Management Protocol Properties dialog box opens.

How to Set Device Management Protocol Properties

Step 1 In the Device Management Protocol Properties dialog box, you must enable connections within the CallRouter Device Management Protocol (DMP) for each Peripheral Gateway (PG) that communicates with the CallRouter—by checking 1, 2, and so forth, up to the number of PGs involved.

Note: These numbers are used as the PG IDs in the Peripheral Gateway Properties dialog box.

Up to 80 PGs can be connected to the CallRouter. Each PG has a device number in the range 1 through 80. Check the boxes for the PG devices you use. When you configure a PG, you must reference a PG device number enabled here.

Warning: A duplexed CallRouter must have at least one PG defined. Only the CallRouter side that has active connections to the majority of the PGs routes calls. (This prevents both Side A and Side B from routing calls simultaneously.) If no PGs are defined, neither side is activated. If necessary, create a PG with no associated peripherals to satisfy this requirement.

Step 2 The **Disconnect warnings** settings determine when the CallRouter reports that a device is disconnected. Accept the default values unless told otherwise by your ICM support provider.

Step 3 Click **Next.**.

The Central Controller Network Interfaces dialog box opens.

See Also

For the Peripheral Gateway Properties dialog box, How to Set Peripheral Gateway Properties (page 61). For information on the DMP configuration for PGs, How to Set Device Management Protocol Properties (page 64). For the Central Controller Network Interfaces dialog box, How to Set Central Controller Network Interfaces (page 28).

How to Set Central Controller Network Interfaces

The Central Controller is the computer or computers running the CallRouter and the Logger.

Step 1 In the Central Controller Network Interfaces dialog box, in the Router Private Interfaces section, you must enter two addresses: one to be used by normal traffic (**A**) and another to be used by high priority traffic (**A high**). You can use either host name or IP address.

Step 2 In the Router Private Interfaces section, if the CallRouter is duplexed, you must enter two addresses for the other side: one to be used by normal traffic (**B**) and another to be used by high priority traffic (**B high**).

If the CallRouter is simplexed, enter **localhost** in both the **B** and **B high** fields.

Step 3 In the Router Visible Interfaces section, you must enter two addresses: one to be used by normal traffic (**A**) and another to be used by high priority traffic (**A high**).

Step 4 In the Router Visible Interfaces section, if the CallRouter is duplexed, you must enter two addresses for the other side: one to be used by normal traffic (**B**) and another to be used by high priority traffic (**B high**).

If the CallRouter is simplexed, enter **localhost** in both the **B** and **B high** fields.

The CallRouter must have two addresses on the private network: one to be used by high priority traffic and another to be used by normal traffic. If the CallRouter is duplexed, each side must have two addresses. Enter the addresses in the appropriate fields of the dialog box. If the CallRouter is simplexed, enter **localhost** in the B fields.

Step 5 If you wish to use the Cisco ICM Quality of Service (QoS) feature for the Router Private Interfaces, click **QoS...** in that section.

The Central Controller Private Link QoS Settings dialog box opens.

Step 6 If you wish to use the Cisco ICM Quality of Service (QoS) feature for the Router Visible Interfaces, click **QoS...** in that section.

The Central Controller Visible Link QoS Settings dialog box opens.

Step 7 If you do not wish to use QoS—or after you have made your QoS settings—click **Next**.

The Check Setup Information window opens.

See Also

As required, How to Set the QoS Feature for the Router Private Interfaces (page 29), How to Set the QoS Feature for the Router Visible Interfaces (page 30), How to Complete CallRouter Setup (page 31).

How to Set the QoS Feature for the Router Private Interfaces

The Central Controller Private Link QoS Settings dialog box comes in two forms.

- If you are installing the CallRouter on Side A of a duplexed system, or you are installing the CallRouter on a simplexed system, you see the Central Controller Private Link QoS Settings (Side A) dialog box.
- If you are installing the CallRouter on Side B of a duplexed system, you see the Central Controller Private Link QoS Settings (Side B) dialog box.

Further, the precise nature of the Side A and Side B forms depends on whether you use Microsoft Packet Scheduler or not; that is, there are actually four forms.

Step 1 In the Central Controller Private Link QoS Settings (Side A) dialog box, check **Enable QoS**. (There is no **Enable QoS** box in the Central Controller Private Link QoS Settings (Side B) dialog box. QoS is enabled on Side B if, and only if, it is enabled on Side A.)

Step 2 Check **Use Packet Scheduler** if you plan to use Microsoft Packet Scheduler.

Leave **Use Packet Scheduler** unchecked if you do not plan to use Microsoft Packet Scheduler.

If **Use Packet Scheduler** is checked for Side A, it must be checked for Side B.

If **Use Packet Scheduler** is unchecked for Side A, it must be unchecked for Side B.

Note: Cisco recommends NOT implementing Microsoft Packet Scheduler for ICM 7.0(0). For more information about ICM QoS, and about this recommendation in particular, refer to the *Pre-Installation Planning Guide for Cisco ICM Enterprise Edition*. If you plan to use Microsoft Packet Scheduler you must install it separately—it is not installed from ICM Setup.

Step 3 Select DSCP priority markings and 802.1p priority tagging, and enter Bandwidth information, as appropriate and allowed—if Packet Scheduler is used, Setup checks that **Total usable bandwidth (Kbps)** is at least 1544 and that the **Bandwidth Percent** values add up to 100.

Note the following differences among the four forms:

- With Packet Scheduler there are only two priority levels (High and Low)—the Medium Priority traffic is marked the same as the Low Priority traffic.
- Bandwidth settings are not enabled on Side B because that information is obtained from Side A.
- The Select Network Interface Card list is used only with Packet Scheduler, in which case a Card must be selected from the display of available Cards.
- When using Packet Scheduler, the same DSCP and 802.1p settings must be used for every ICM instance that uses a given Network Interface Card. Record the settings you use to make sure that this rule is followed.
- When not using Packet Scheduler, the Side B dialog box has no fields enabled because the information is obtained from Side A.

Step 4 Click **OK**, which accepts the information that you entered, and returns you to the Central Controller Network Interfaces dialog box.

See Also

For the Central Controller Network Interfaces dialog box, How to Set Central Controller Network Interfaces (page 28).

How to Set the QoS Feature for the Router Visible Interfaces

Step 1 In the Central Controller Visible Link QoS Settings dialog box, either check **Use Packet Scheduler**, or click **Cancel**. (There is no **Enable QoS** box in the Central Controller Visible Link QoS Settings dialog box. QoS is enabled if, and only if, it is enabled for the PG Visible Link QoS Settings. Further, when not using Packet Scheduler, no fields are enabled because the information is obtained from the PG Visible Link QoS Settings.)

Step 2 If you have checked **Use Packet Scheduler**, select DSCP priority markings and 802.1p priority tagging as appropriate and allowed. With Packet Scheduler there are only two priority levels (High and Low)—the Medium Priority traffic is marked the same as the High Priority traffic.

Note that the bandwidth settings for the Central Controller are determined by the bandwidth settings for the PG; therefore, the bandwidth settings are disabled here.

Step 3 Click **OK**, which accepts the information that you entered, and returns you to the Central Controller Network Interfaces dialog box.

See Also

For the bandwidth settings for the PG, How to Set the QoS Feature for the PG Visible Interfaces (page 67). For the Central Controller Network Interfaces dialog box, How to Set Central Controller Network Interfaces (page 28).

How to Complete CallRouter Setup

Step 1 In the Check Setup Information window, ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the **Back** button.

Step 2 When the settings are correct, click **Next** to begin copying files.

The copying process may take several minutes to complete. You can continue with other work while Setup operates in the background.

Step 3 If Setup successfully copies all the files, it displays the final screen and asks whether you want to start the ICM Node Manager now. Do not start the Node Manager until you have completed the entire ICM installation.

Step 4 Click **Finish** to exit Setup (and optionally start the Node Manager).

If you choose to start it, the Node Manager automatically starts the other ICM processes on the CallRouter.

Chapter 3

Logger Setup

Before You Install a Logger

The Logger is the interface between the ICM software and the Microsoft SQL Server database. As the ICM software collects performance and monitoring information about the system, it passes the information to the Logger for storage in a central relational database. The database manager on the Logger maintains statistics and data for use in monitoring and reporting. The Logger also forwards historical information to the Historical Data Server (HDS). Although the Logger represents a single node, it consists of two processes operating in parallel: one process handles configuration data and the other handles historical data.

Before you install the Logger software, the Microsoft Windows operating system—including SNMP and (for Windows 2003) WMI—and Microsoft SQL Server (for version specifics refer to the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials*) must be installed on the computer, you must have set up the Windows Active Directory services for ICM software, and you must have set up at least one ICM instance.

This chapter explains how to install the Logger software and perform some basic configuration. For this configuration, you must know the private network addresses of the CallRouter machines and, for a duplexed configuration, the addresses of the Logger on the other Side. (You can use either host names or IP addresses.)

The Logger and CallRouter are typically on separate computers. However, in small contact center configurations they can both be on the same computer.

To set up a Logger, you must first install the Logger software and then create the Logger's database.

See Also

Before You Install an ICM Component (page 13); How to Add an Instance (page 21).

How to Install a Logger

How to Add a Logger Component

Step 1 In the Cisco ICM Setup dialog box, in the left column under ICM Instances, select an instance.

Step 2 Click **Add** in the Instance Components section.

The ICM Component Selection dialog box opens.

Step 3 Click **Logger**.

The Logger Properties dialog box opens.

See Also

Cisco ICM Setup dialog box (page 19); ICM Component Selection dialog box (page 24).

How to Set Logger Properties

The following task describes how to set the Logger properties.

Step 1 In the Logger Properties dialog box, check **Production mode** and **Auto start at system startup** unless you are specifically told otherwise by your ICM support provider. This ensures that the Logger can restart itself automatically if necessary.

Note: However, set the Auto Start feature only **after** your ICM installation is otherwise complete. The server may need to be rebooted a number of times during installation, and problems could occur if the node starts before patches and/or databases are applied.

Step 2 Check the **Duplexed Logger** option if you are configuring redundant Logger machines.

Step 3 If one or more admin sites will use an Historical Data Server (HDS), check the **Historical Data Replication** option. This enables the Logger to forward historical data to an HDS database at an admin site.

Step 4 Do not check the **No system reboot on error** option if the machine runs only a single Logger component and no other critical applications. This will allow the ICM to reboot the machine when necessary to recover from errors or when the Logger specifically requests a reboot.

If multiple instances of the Logger run on the same physical machine or if other critical processes run on the machine, check this option. If you choose this option, you may need to manually recover from some failures.

Step 5 DO NOT CHECK the **No system reboot on request** option unless specifically told to do so by your ICM support provider. Checking this option prevents the Logger from rebooting even if it detects a serious system-wide problem.

Step 6 Choose a **Logger Type** that corresponds to your ICM system (**Standard** for Enterprise systems; **NAM** or **CICM** for Hosted systems).

Step 7 If the Logger will be duplexed, specify which **Side** you are installing: Side A or Side B. If the Logger will be simplexed, choose Side A

Step 8 Choose the local **Drive** on which you want to install the software.

Note: Be sure to note the drive you are using for future reference, since this information is required when applying software patches.

Step 9 Choose the **Language** from the list.

Step 10 Click Next.

Setup loads any current installation settings and then—if you have selected either Standard or CICM as your Logger Type—the Logger Component Properties dialog box opens.

If you have selected **NAM** as your Logger Type, the NAM Properties dialog box opens—refer to the *Setup and Configuration Guide for Cisco ICM Hosted Edition* .

How to Set Logger Component Properties

Note: The Cisco Technical Assistance Center (TAC) no longer supports new customers with the Remote Monitoring Suite (RMS). Cisco no longer documents nor sells TAC monitoring of ICM systems via RMS. Refer to your MSA/Master Service Agreement for more information. However, your ICM support/service provider may support RMS.

Step 1 In the Logger Component Properties dialog box, to enable the DDSN, in the Customer support section, check the **Phone home** option and then click **Configure**.

The Phone Home Configuration dialog box opens.

Note: Refer to the *ICM Administration Guide for Cisco ICM Enterprise Edition* for more information on DDSN.

Step 2 If you do not wish to use Phone Home—or after you have configured Phone Home—check the **Enabled** box in the Outbound Option section and click **Configure** if you are using Cisco Outbound Option.

The Outbound Option Configuration dialogue box opens.

If you do not wish to use Outbound Option—or after you have configured Outbound Option—continue with the next step.

Step 3 The central ICM database resides on the Logger machine. The **Purge** button lets you modify advanced settings that determine how the Logger manages the database.

To prevent the central ICM database from growing to infinity, the Logger must periodically purge old data from historical tables. By default, the Logger runs a purge every day during which it deletes any historical data that is greater than 100 days old. You can also configure the Logger to run a daily purge adjustment when the database fills to a defined percentage (the default is 80%). The Logger also runs a purge any time the database becomes more than 95% full.

You can change when the purge job executes and how long you want the Logger to retain data for each historical table. To modify these settings, click the **Purge** button.

The Purge Configuration dialog box opens.

Step 4 Click **Next**.

The Network Interface Properties dialog box opens.

See Also

For the Phone Home Configuration dialog box, How to Set the Phone Home Configuration (page 36). For the Outbound Option Configuration dialogue box, How to Set the Outbound Option Configuration (page 37). For the Purge Configuration dialog box, How to Set the Purge Configuration (page 38). For the Network Interface Properties dialog box, How to Set Network Interface Properties (page 36).

How to Set Network Interface Properties

Step 1 Specify the private network interfaces for the **A** and (if applicable) **B** sides of the CallRouter (**Router private interfaces**) and Logger (**Logger private interfaces**). You can use either the host name or the IP address.

Step 2 Click **Next**. The Check Setup Information window opens.

See Also

For the Check Setup Information window, How to Complete Logger Setup (page 38).

How to Set the Phone Home Configuration

For more information on this feature refer to the *ICM Administration Guide for Cisco ICM Enterprise Edition* and the Remote Monitoring Suite documentation.

Note: The ICM software cannot be installed on the same machine that is running the Listener software.

Step 1 In the Phone Home Configuration dialog box, in the **CSFS** (Customer Support Forwarding Service) **configuration** section, enter the **Customer name** (typically a three- or four-letter value) and **Site name** (for duplexed components, this value must be unique for each side; for example, LoggerA or LoggerB). Also specify the **Suppression limit**, which is the maximum number of times any one event can be repeated within the Suppression Time; and the **Suppression time**, which is the interval, in minutes, during which the Suppression Limit applies.

Step 2 In the **Contacting Support** section, specify in **Heartbeat interval** the number of minutes between CSFS test messages to your support provider, in **User ID** the login name used by DTP when connecting to the support machine, and in **Password** the password used by DTP when connecting to the support machine.

Step 3 In the **Contacting Support** section, specify how to contact the **Primary Listener**. Either specify the telephone number for a RAS connection in the **Phone number** field or check the **Send data over local network** option for a direct network connection. Modify the **Import directory** value by replacing the string customer_name with the actual customer name. Set **Import system name** and **Import domain** to point to the machine running the Listener. If you have a backup Listener, enter the phone and import information for the **Backup Listener**.

Step 4 In the **Serial feed configuration** section, check the **Enable** box to enable the ICM Serial Feed facility. This facility allows you to monitor ICM events locally through a serial port. Complete the **Comport** field with the port on the Logger through which you want to receive events. This port must be after the port used by DTP. By default, DTP uses COM1 and the Serial Feed facility uses COM2. Enter the **Pipe name** through which the Serial Feed facility receives events. This must always be set to CSFSEventFeed. Set the **Speed** at which the listening device can receive events. The default is 9600.

Step 5 Click **OK**, which accepts the information that you entered, and returns you to the Logger Component Properties dialog box.

See Also

For the Logger Component Properties dialog box, How to Set Logger Component Properties (page 35).

How to Set the Outbound Option Configuration

Step 1 In the Outbound Option Configuration dialog box, in the **SQL server system** field, enter the host name or IP address of the machine that has the SQL database.

Step 2 Enter the **Heartbeat** for the connection. The default is usually acceptable.

Note: Refer to the *Outbound Option Setup and Configuration Guide for Cisco ICM/IPCC Enterprise & IPCC Hosted Editions* for more information.

Step 3 Click **OK**, which accepts the information that you entered, and returns you to the Logger Component Properties dialog box.

See Also

For the Logger Component Properties dialog box, How to Set Logger Component Properties (page 35).

How to Set the Purge Configuration

Step 1 To change the length of time that the Logger retains data in a table, select that **Table** and enter a new value for **Retention period**.

Step 2 You can also change the **Purge schedule** for the daily purge job.

Step 3 In addition, you can specify whether you want a purge to execute automatically when the database reaches the **Automatic** and/or **Daily** purge thresholds. Specify these thresholds as the percentage of the database that becomes full.

Step 4 Click **OK**, which accepts the information that you entered, and returns you to the Logger Component Properties dialog box.

See Also

For the Logger Component Properties dialog box, How to Set Logger Component Properties (page 35).

How to Complete Logger Setup

Step 1 In the Check Setup Information window, ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the **Back** button.

Step 2 When the settings are correct, click **Next** to begin copying files.

The copying process may take several minutes to complete. You can continue with other work while Setup operates in the background.

Step 3 If Setup successfully copies all the files, it displays the final screen and asks whether you want to start the ICM Node Manager now. Do not start the Node Manager until you have completed the entire ICM installation

Step 4 Click **Finish** to exit Setup (and optionally start the Node Manager).

If you choose to start it, the Node Manager automatically starts the other ICM processes on the Logger.

Note: When you have completed the Logger installation, you must use the ICMDBA utility to create the Logger database.

Creating the Central Database

You must create a database for each Logger. To create the database and determine the appropriate size of the database, run the ICM Database Administration (ICMDBA) tool. This tool is installed on each ICM component that has an installed database (ICMDBA is in the \icm\bin directory) and on each Admin Workstation.

Refer to the *ICM Administration Guide for Cisco ICM Enterprise Edition* for more information on using the ICMDBA tool.

Chapter 4

Admin Workstation Setup

Before Installing an Admin Workstation

The Admin Workstation (AW) is the human interface to the ICM software. It serves as a control console from which you can monitor agent and contact center activity and change how the ICM software routes contacts. For example, you can use the Admin Workstation to configure the ICM contact center data and to create routing scripts. Admin Workstations can be located anywhere, as long as they have LAN, WAN, or dial-up connections to the ICM software. There are two AW options, Real-time Distributor and Client; these options are discussed below.

Before you install the Admin Workstation (AW) software, the following must have been done on the computer:

- Installed Microsoft Windows operating system (for version specifics refer to the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials*)—including SNMP and (for Windows 2003) WMI.
- Installed Microsoft SQL Server database, if it is not a Client AW (for version specifics refer to the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials*).
- Set up the Windows Active Directory services for ICM software.
- Set up at least one ICM instance.
- If you plan to install WebView, be aware that it can be installed only on a machine where there is a Primary, HDS-enabled, Real-time Distributor AW, or on its own machine.

  For information on installing WebView, see the *WebView Installation and Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

  Admin Workstations (AWs) may be part of the Central Controller domain or in another domain. If the AW is in another domain, you must establish a two-way trust relationship between the AW and Central Controller domain.

Install the AW software on a node separate from other ICM software. The node can be located on any LAN that has WAN access to the Central Controller.

You have two options when installing the Admin Workstation software:

- Client (no Real-time Distributor)
- Real-time Distributor

The following table summarizes the difference between Real-time Distributor and Client-only Admin Workstations.

Table 6: Distributor vs. Client Admin Workstation

	Distributor Admin Workstation	Client Admin Workstation
Types	Standard	Standard
Applications	Full complement, depending on type	Full complement, depending on type
Local Database	Yes	No
Windows Service	Cisco ICM Distributor	N/A
Background Processes	configlogger, histlogger, rtclient, rtdist, updateaw	N/A
Optional Processes	schman, replication	N/A

Note: There must be at least one Distributor Admin Workstation at a site before a Client Admin Workstation can be installed.

If you have more than one Admin Workstation on a single LAN, then only one of these machines needs to receive the real-time feed—which contains real-time monitoring data—from the Central Controller. That machine (a Distributor AW) acts as the real-time distributor and passes the real-time data to other (Client) Admin Workstations at the site. If possible, configure two machines at the site as real-time distributors: one as the primary and the other as the secondary (backup) distributor.

Optionally, you can configure a real-time distributor AW to also act as a Historical Data Server (HDS). The Logger then forwards historical data to a special database on the distributor. Admin Workstations at the local site can then access historical data from the distributor rather than from the central database. (If you intend to install and use WebView for historical reporting, you **must** enable HDS on the distributor.)

Note: For a Historical Data Server, you must first install the Admin Workstation software without the HDS option enabled. Then create the HDS database and run Setup locally to enable the HDS.

Also, a WebView database **must** reside on a real-time distributor AW, although you can choose which distributor to put it on.

Refer to the *ICM Administration Guide for Cisco ICM Enterprise Edition* for information on setting up the HDS.

See Also

Before You Install an ICM Component (page 13); How to Add an Instance (page 21).

How to Install an Admin Workstation

How to Add an Admin Workstation Component

Step 1 In the Cisco ICM Setup dialog box, in the left column under ICM Instances, select an instance.

Step 2 Click **Add** in the Instance Components section.

The ICM Component Selection dialog box opens.

Step 3 Click **Admin Workstation**. .

The Admin Workstation Properties dialog box opens.

See Also

Cisco ICM Setup dialog box (page 19); ICM Component Selection dialog box (page 24).

How to Set Admin Workstation Properties

Step 1 In the Admin Workstation Properties dialog box, select the type of **Admin Workstation Configuration**:

Client (No Real-time Distributor). This configuration includes standard Admin Workstation applications, such as Script Editor and ICM Configuration Manager. It does not include the processes that directly manage a database.

Real-time Distributor. This configuration includes the real-time distributor and real-time client processes, and all processes that directly manage the local database. A single distributor Admin Workstation can run the distributor processes for multiple customers simultaneously. However, it can run client applications (such as Script Editor and ICM Configuration Manager) for only one customer at a time. Use AW Select to change the customer.

Step 2 Select the **AW Type**.

For ICM Enterprise Edition, select **Standard**.

For ICM Hosted Edition, select one of the other choices (**Limited AW, Network AW (NAM), Network AW (CICM)**). Refer to the *Setup and Configuration Guide for Cisco ICM Hosted Edition* for information on these AW types, and for specifics on installing them. The following instructions always assume that you have chosen **Standard**.

Step 3 Always choose **Production Mode** for the Node Manager unless you are specifically told otherwise by your ICM support provider.

Step 4 Choose the **Target drive** on which you want to install the software.

Note: Be sure to note the drive you are using for future reference, since this information is required when applying software patches.

Step 5 Choose the **Language** from the drop-down list. This determines which online help files are installed.

Note: If you are setting up a Distributor AW, and have already installed WebView (and chosen the language) on the same machine as this Distributor AW, the Language field has the value you selected when installing WebView. You may change the language if you wish, but a warning will come up informing you that you are overriding the previous selection, and asking you to confirm if you want to do that.

The language you select also determines the date format that is used in reports. The following table describes date formats for each language.

Table 7: Report Date Format for Languages

AW Setup Language	WebView UI	Date Format in Reports
English (USA)	English	MM/DD/YYYY
English (UK)	English	DD/MM/YYYY
French (Canada)	French	YYYY/MM/DD
French (France)	French	DD/MM/YYYY
German	English	DD/MM/YYYY
Spanish	English	DD/MM/YYYY
Chinese (Simplified)	Chinese	YYYY/MM/DD
Japanese	Japanese	YYYY/MM/DD
Korean	Korean	YYYY/MM/DD

Customers who want to run ICM on a Windows operating system which is not localized in one of these languages, but who want to use the DD/MM/YYYY date format, must select UK English, France French, German, or Spanish as the AW Setup language.

Note: The character set used in ICM 7.0(0) databases is determined by the collation designator of SQL 2000 Server. ICM 7.0(0) supports the following Collation Designators: Latin1, Japanese, Chinese_PRC, and Korean_Wansung. ICM 7.0(0) supports ASCII characters only—except for the Agent Names, Description, and Reason Code fields. Validation rules do not apply to these three fields. This means that a supervisor running a report in English, based on data from a call center in Japan, sees reporting data in English except for these three fields, which would appear in Japanese. Data is stored in the AW and HDS databases in native character sets.

Step 6 Click **Next**.

If you selected **Real-time Distributor** in the Admin Workstation Configuration section, the Real-time Distributor Node Properties dialog box opens.

If you selected **Client (No Real-time Distributor)** in the Admin Workstation Configuration section, the Admin Workstation Client Properties dialog box opens.

See Also

For AW Select, Cisco Admin Workstation Program Group (page 102). For the Real-time Distributor Node Properties dialog box, How to Set Real-time Distributor Node Properties (page 45). For the Admin Workstation Client Properties dialog box, How to Set Admin Workstation Client Properties (page 47).

How to Set Real-time Distributor Node Properties

The Real-time Distributor Node runs as a Windows service and manages several ICM processes (including the local Logger process, real-time client, and real-time distributor).

Step 1 In the Real-time Distributor Node Properties dialog box, you can choose to have the Node Manager start automatically each time you start the computer. If you do not choose the **Auto start** option then you must start the Node Manager manually before you can use the ICM tools.

Note: Set the Auto Start feature only **after** your ICM installation is otherwise complete. The server may need to be rebooted a number of times during installation, and problems could occur if the node starts before patches and/or databases are applied.

Step 2 Agent Re-skilling (an IPCC-only feature) allows a supervisor to change the skill groups assigned to an agent and have that change become effective immediately (otherwise the re-assignment becomes effective only after the agent logs out and then logs back in). Check **Agent Re-skilling Web Tool** if you want this feature and the tool that is used in association with this feature. Refer to the tool's online help for operating instructions. (Checking Agent Re-skilling Web Tool automatically checks CMS Node—see below.)

Note: IIS must be installed in order to enable Agent Re-skilling.

Step 3 Check **CMS Node** to enable the Configuration Management System node. This engine can access the ICM configuration and manages connectivity and resources for applications, such as the Cisco Web Collaboration (including Collaboration Server) option and Cisco E-Mail Manager option, that connect to the ICM platform. This box is automatically checked if you have checked Agent Re-skilling.

Step 4 Check **Internet Script Editor Server** if you want to download the Internet Script Editor software.

For new installations, you must access a web page on the ICM distributor to download the software. The Internet Script Editor software is a self-extracting archive that you must download and run.

You must have write access to the chosen install directory, and to registry branch HKEY_LOCAL_MACHINE.

Note: Refer to the *ICM Scripting and Media Routing Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for more information on the Internet Script Editor.

Step 5 Click **Next**.

The Real-time Distributor Properties dialog box opens.

How to Set Real-time Distributor Properties

Step 1 In the Real-time Distributor Properties dialog box, enter the **Admin site name** and indicate if this the **Secondary distributor** for the site (if it is the Primary distributor, leave the box unchecked).

When naming AWs at the same site, use the same site name for all Distributor and Client AWs at the site.

Step 2 Indicate the **Central controller preferred side**, that is, indicate the side of the Central Controller from which you prefer to receive real-time data.

This is important, for example, if the Admin Workstation is collocated with one side of the Central Controller. You can prevent unnecessary traffic on the wide area network by choosing the local side of the Central Controller as the preferred side.

If this is a simplexed system, the preferred side must be **Central controller side A**.

Step 3 Check **WebView Database** if you want a WebView database to reside on this Admin Workstation—refer to the *WebView Installation and Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for additional information.

Note: If you intend to install WebView on this Distributor AW machine; or if you intend to install WebView on another machine, but configured to point to this Distributor AW machine; then this Distributor AW machine must be HDS-enabled.

Step 4 Check **Historical Data Server** if you intend to use the HDS.

Note: If you want to configure the AW as a Historical Data Server, do **not** check **Historical Data Server** the first time you run Setup. For a Historical Data Server, you must first install the Admin Workstation software without the HDS option enabled. Then create the HDS database and run Setup locally to enable the HDS. (If you check this box and no HDS database has yet been installed, inappropriate values will be set that will not be reset by simply creating the database later. Conversely, the HDS database cannot be created on a Distributor AW until the Distributor AW has been set up.)

Refer to the *ICM Administration Guide for Cisco ICM Enterprise Edition* for more information on configuring the HDS.

Step 5 Check **Partitioning** to install the ICM's optional partitioning software. This allows you to partition data in the ICM database and selectively limit access that groups of users have to specific data.

Refer to the *ICM Administration Guide for Cisco ICM Enterprise Edition* for more information on ICM Partitioning.

Note: Partitioning is only supported for customers using ICM Enterprise Edition. It is not supported in ICM Hosted Edition, IPCC Enterprise Edition, or IPCC Hosted Edition.

Step 6 Each Real-time Distributor Admin Workstation must have a Microsoft SQL Server database. Specify the **SQL Server Drive**.

Step 7 In the **Central Controller** section, enter the enter the IP addresses or host names of the CallRouter machines for each side and the Logger machines for each side. In the case of a simplexed CallRouter/Logger, enter **localhost** for the B side address.

Step 8 Click **Next.**

The Admin Workstation Client Properties dialog box opens.

How to Set Admin Workstation Client Properties

Step 1 In the Admin Workstation Client Properties dialog box, in the **Real Time Distributors** section, specify the Admin Workstations that will serve as the primary and (if used) secondary real-time distributors for the site.

If you are setting up a real-time distributor AW, one of these fields will be greyed out and contain the information that you entered in the preceding Real-time Distributor Properties dialog box.

Note: If you are configuring an HDS, be sure that you indicate it as the primary distributor. Otherwise your WebView reports will go to your Logger machine rather than to your HDS machine.

Every Admin site must have at least one—and preferably two—Admin Workstations serve as real-time distributors. At any time, one distributor at each site receives real-time data directly from the Central Controller. Other Admin Workstations receive their real-time data from the distributor

For a description of the real-time architecture and advice about choosing Admin Workstations to act as distributors, refer to the *Pre-Installation Planning Guide for Cisco ICM Enterprise Edition*.

Warning: All Admin Workstations for a site must specify the same two machines as the primary and secondary real-time distributors.

Step 2 Check the **Workforce Management** box if you want to install ICM's optional Cisco Schedule Link product. This allows you to import scheduling information from a third-party workforce management system.

Step 3 Check the **Outbound Option Support** box to enable the Outbound Option configuration tools in the ICM Configuration Manager.

Step 4 Click **Next**.

The Check Setup Information window opens.

See Also

For the Real-time Distributor Properties dialog box, How to Set Real-time Distributor Properties (page 46).

How to Complete Admin Workstation Setup

Step 1 In the Check Setup Information window, ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the **Back** button.

Step 2 When the settings are correct, click **Next** to begin copying files.

Step 3 If Setup successfully copies all the files, it displays the final screen and asks whether you want to start the ICM Node Manager now. Do not start the Node Manager until you have completed the entire ICM installation.

Step 4 Click **Finish** to exit Setup (and optionally start the Node Manager).

If you choose to start it, the Node Manager automatically starts the other ICM processes on the Admin Workstation: the local logger process, the real-time client, and (if the Admin Workstation is the active distributor) the real-time distributor.

An ICM Admin Workstation icon appears on your desktop.

Admin Workstation Databases

When you install a Distributor Admin Workstation, ICM Setup automatically sizes and creates a local database on the machine. Because this database is constantly overwritten by new data, the database size remains fairly constant. You normally do not need to resize the Distributor

AW real-time database. If you do need to resize the Distributor AW database, you can do so using the ICM Database Administration (ICMDBA) tool.

After you install the AW, you must (if you have checked the Historical Data Server option) create an HDS database on a real-time Distributor Admin Workstation. The same considerations that affect the size of the central database also affect the size of the HDS database.

For instructions on installing the HDS database with ICMDBA, refer to the *ICM Administration Guide for Cisco ICM Enterprise Edition*.

Chapter 5

Network Interface Controller Setup

Before Setting Up a Network Interface Controller

The Network Interface Controller (NIC) connects the ICM software to the IXC signaling network. The NIC receives a route request from the signaling network for each incoming call and passes the request to the ICM software. The ICM software responds with routing information (a routing label), which the NIC passes back to the IXC signaling network. NICs are implemented as software on the same server as the CallRouter.

Before you can complete the installation of a Network Interface Controller (NIC), you must create configuration records in the ICM database. To create these configuration records you must have installed a CallRouter, a Logger, and an Admin Workstation.

This chapter discusses:

- Running the ICM Configuration Manager on an Admin Workstation to create configuration records for NICs.
- Running the local ICMSetup on the CallRouter machine to set up NICs on that machine.

How to Make NIC Configuration Changes

How to Create Necessary Configuration Records

The following discusses how to create the necessary configuration records.

Step 1 Start the ICM AW, Logger and Router services.

Step 2 Start the Configuration Manager on the Admin Workstation. To start the Configuration Manager, double-click on its icon within the ICM Admin Workstation program group.

For information about the Configuration Manager, see the *ICM Configuration Guide for Cisco ICM Enterprise Edition*.

Step 3 To create the appropriate configuration records for a NIC, run the NIC Explorer from the ICM Admin Workstation Group directory.

The following records are created with these options:

- Logical_Interface_Controller (one for each NIC)
- Physical_Interface_Controller (one or more for each NIC)
- Routing_Client (one or more for each NIC)

Step 4 You can view and edit the individual records through the Configuration Manager. For example, to view a Logical_Interface_Controller record, choose **Logical Interface Controller** from the Requesters menu. The Configuration Manager displays a list of records. To view a specific record, double-click on it, or select it and click the **Update** button.

To complete the setup for NICs, you need to get a few specific values from the records you create in the Configuration Manager, namely, the Physical Controller ID from each Physical_Interface_Controller record.

How to Configure Specific NICs

The Network Interface Controllers (NICs) run as subcomponents of the CallRouter. After you have defined the NICs in the Configuration Manager, you must run ICMSetup on the CallRouter to complete the NIC configuration.

To do this:

Step 1 Run the local version of ICM Setup that was installed on the CallRouter machine. The executable is ICMSetup.exe in the \icm\bin directory.

Step 2 In the ICM Instance section of the Cisco ICM Setup dialog box, select the desired instance.

Step 3 In the Instance Components section of the Cisco ICM Setup dialog box, select the Router and click **Edit**.

Step 4 Proceed to the Router Component Properties dialog box, as described in Chapter 2, "CallRouter Setup".

Step 5 In the Router Component Properties dialog box, indicate whether you want to enable one or several of the NICs by checking the appropriate boxes.

Step 6 To configure a particular NIC, click **Configure...** for that checked NIC.

Step 7 The appropriate NIC Properties dialog box opens.

The following subsections describe how to configure each of the ICM NICs.

See Also

Cisco ICM Setup dialog box (page 19). For the Router Component Properties dialog box, How to Set Router Component Properties (page 27)

How to Configure the AT&T NIC

Step 1 In the AT&T NIC Properties dialog box, enter the **Physical controller ID** value from the Configuration Manager.

Step 2 For the other fields in the top part of the dialog box, the default values are usually appropriate.

Use the Gateway Properties section to enter values for each connection between the NIC and the AT&T Gateway.

Step 3 In the Description field, enter any descriptive text you want for the connection to the AT&T Gateway.

Step 4 In the Address field, enter the IP address or hostname for the AT&T Gateway.

Step 5 In the Port field, enter the TCP port to use for connection to the AT&T Gateway.

How to Configure the AUCS INAP NIC

Step 1 In the Unisource NIC Properties dialog box, enter the **Physical controller ID** value from the Configuration Manager.

Step 2 For the other fields in the top part of the dialog box, the default values are usually appropriate.

Use the Gateway Properties section to enter values for each connection between the NIC and the Unisource INAP Gateway.

Step 3 In the **Description** field, enter any descriptive text you want for the connection to the Unisource INAP Gateway.

Step 4 In the **Address** field, enter the IP address or hostname for the Unisource INAP Gateway.

Step 5 In the **Port** field, enter the TCP port to use for connection to the Unisource INAP Gateway.

How to Configure the CAIN NIC

Step 1 In the CAIN NIC Properties dialog box, enter the **Physical controller ID** value from the Configuration Manager.

Step 2 For the other fields in the top part of the dialog box, the default values are usually appropriate.

Use the Gateway Properties section to enter values for each connection between the NIC and the CAIN Gateway.

Step 3 In the **Description** field, enter any descriptive text you want for the connection to the CAIN Gateway.

Step 4 In the **Address** field, enter the IP address or hostname for the CAIN Gateway.

Step 5 In the **Port** field, enter the TCP port to use for connection to the CAIN Gateway.

How to Configure the CRSP NIC

Step 1 In the CRSP NIC Properties dialog box, enter the **Physical controller ID** value from the Configuration Manager.

Step 2 For the other fields in the top part of the dialog box, the default values are usually appropriate.

Step 3 Use the SCP/VRU Clients section to enter values for the SCP.

Step 4 Check the **Enabled** box to enable an SCP. In the Description field, enter a description of the SCP.

Step 5 In the **Description** field, enter a description of the SCP.

Step 6 In the **IP Address** field, enter the IP address of the SCP.

Step 7 In the **Client ID** field, enter the ID of the SCP.

If there are multiple SCPs using the same IP address, the Client ID must be unique for each SCP at the address.

How to Configure the CWC NIC

Step 1 In the CWC NIC Properties dialog box, enter the **Physical controller ID** value from the Configuration Manager.

Step 2 For the other fields in the top part of the dialog box, the default values are usually appropriate.

Use the Gateway Properties section to enter values for each connection between the NIC and the CWC Gateway.

Step 3 In the **Description** field, enter any descriptive text you want for the connection to the CWC Gateway.

Step 4 In the **Address** field, enter the IP address or hostname for the CWC Gateway.

Step 5 In the **Port** field, enter the TCP port to use for connection to the CWC Gateway.

How to Configure the GKTMP NIC

Step 1 In the GKTMP NIC Properties dialog box, use the Network Interface Controller Properties to apply settings to the NIC device.

Step 2 In the **Local IP Address** field, enter the IP address or host name for the GKTMP NIC.

Step 3 In the **Listening TCP Port Number** field, enter the port number that the GKTMP NIC will use to listen for TCP/IP connections.

Step 4 In the **Physical Controller ID** field, enter the Integer identifier for the GKTMP NIC from the Physical_Interface_Controller table in the ICM database.

Step 5 In the **Maximum number of Sessions** field, enter the number of sessions you want the NIC to support. The GKTMP NIC supports up to a maximum of 64 sessions.

Step 6 In the **RAS Port Number** field, enter the port number used in the LCF response message for the Registration, Admission and Status protocol address. The default is 1719.

Step 7 Check the **Provide distinct LRQ destInfo alias address space** box if you want the GKTMP NIC to add a special prefix character to all LRQ destinationInfo aliases before they go to the NAM router.

Step 8 Check the **Cycle through alternate EP selections** box to enable the GKTMP NIC to cycle alternate EP selections. A maximum of ten endpoint transport addresses are configurable in the NAM.

How to Configure the INCRP NIC

Refer to the *Setup and Configuration Guide for Cisco ICM Hosted Edition* for information on configuring the INCRP NIC.

How to Configure the MCI NIC

Step 1 In the MCI NIC Properties dialog box, enter the **Physical controller ID** value from the Configuration Manager.

Step 2 Typically, you do not need to change any other values in this dialog box. The first field is initialized to the high priority, private network IP address of the CallRouter machine. The other values are standard defaults for all MCI NICs.

How to Configure the Nortel NIC

Step 1 In the Nortel NIC Properties dialog box, enter the **Physical controller ID** value from the Configuration Manager.

Step 2 For the other fields in the top part of the dialog box, the default values are usually appropriate.

Step 3 In the bottom part of the dialog box, fill in the specific information for each network SCP that communicates with the NIC.

How to Configure the NTL NIC

Step 1 In the NTL NIC Properties dialog box, enter the **Physical controller ID** value from the Configuration Manager.

Step 2 For the other fields in the dialog box, the default values are usually appropriate.

How to Configure the Sprint NIC

Step 1 In the Sprint NIC Properties dialog box, enter the **Physical controller ID** value from the Configuration Manager.

Step 2 Set the **Number SCPs** field to 4.

Step 3 Typically, you do not need to change any other values in this dialog box. The **Number links per SCP** is standard for all Sprint NICs. Do not change the values of the other fields unless told to do so by your ICM support provider.

How to Configure the SS7IN NIC

Step 1 In the SS7IN NIC Properties dialog box, enter the **Physical controller ID** value from the Configuration Manager.

Step 2 For the other fields in the top part of the dialog box, the default values are usually appropriate.

Use the Gateway Properties section to enter values for each connection between the NIC and the SS7IN Gateway.

Step 3 In the **Description** field, enter any descriptive text you want for the connection to the SS7IN Gateway.

Step 4 In the **Address** field, enter the IP address or hostname for the SS7IN Gateway.

Step 5 In the **Port** field, enter the TCP port to use for connection to the SS7IN Gateway.

How to Configure the Stentor NIC

Step 1 In the Stentor NIC Properties dialog box, enter the **Physical controller ID** value from the Configuration Manager.

Step 2 For the other fields in the top part of the dialog box, the default values are usually appropriate.

Step 3 In the bottom part of the dialog box, fill in the specific information for each network ATfG that communicates with the NIC.

How to Configure the TIM INAP NIC

Step 1 In the TIM INAP NIC Properties dialog box, enter the **Physical controller ID** value from the Configuration Manager.

Step 2 For the other fields in the top part of the dialog box, the default values are usually appropriate.

Use the Gateway Properties section to enter values for each connection between the NIC and the TIM INAP Gateway.

Step 3 In the **Description** field, enter any descriptive text you want for the connection to the TIM INAP Gateway.

Step 4 In the **Address** field, enter the IP address or hostname for the TIM INAP Gateway.

Step 5 In the **Port** field, enter the TCP port to use for connection to the TIM INAP Gateway.

Chapter 6

Peripheral Gateway Setup

Before Installing a Peripheral Gateway

Each contact center device (ACD, PBX, or IVR/VRU) communicates with ICM software through a Peripheral Gateway (PG). The PG reads status information from the device and passes it back to the ICM software. The PG runs one or more Peripheral Interface Manager (PIM) processes, which are the software components that communicate with proprietary ACD and IVR/VRU systems.

Note: A single PG can support ACD PIMs, VRU PIMs, and Media Routing PIMs, though the ACD PIMs must all be of the same kind and the VRUs must all be of the same kind.

Before you install a Peripheral Gateway (PG), the Windows operating system (for version specifics refer to the *Cisco Intelligent Contact Management Software Release 7.0(0) Bill of Materials*)—including SNMP and (for Windows 2003) WMI—must be installed on the computer, you must have set up the Windows Active Directory services for ICM software, and you must have set up at least one ICM instance.

Further, before you can complete the installation of a Peripheral Gateway, you must create configuration records in the ICM database. To create these configuration records you must have installed a CallRouter, a Logger, and an Admin Workstation.

To configure a PG, you must know the visible network addresses for the CallRouter machines. If the PG is duplexed, you must know the visible and private network addresses of its duplexed peer.

For each PG, you must have defined a Logical_Interface_Controller record, a Physical_Interface_Controller record, and a Peripheral record for each PIM you intend to configure—though at least one Peripheral record is necessary. (Configure ICM creates these records automatically if you choose Configure a PG using the PG Explorer.)

Note: ICM software restricts running more than two PGs of the same instance on a single machine at the same time.

See Also

Before You Install an ICM Component (page 13); How to Add an Instance (page 21).

How to Make PG Configuration Changes

The following discusses how to create the necessary configuration records.

Step 1 Start the ICM Router, Logger, and AW services (using the **ICM Service Control** icon on your desktop).

Step 2 Start the Configuration Manager on the Admin Workstation. To start the Configuration Manager, double-click on its icon within the ICM Admin Workstation program group.

Note: For information about the Configuration Manager, refer to the *ICM Configuration Guide for Cisco ICM Enterprise Edition*.

Step 3 To create the appropriate configuration records for a PG, run the PG Explorer in Configuration Manager.

The following records are created with these options:

- Logical_Interface_Controller (one for each PG)
- Physical_Interface_Controller (one for each PG)
- Peripheral (at least one for each PG)
- Routing_Client (one or more for each PG that uses Post-Routing)

Step 4 You can view and edit the individual records through the Configuration Manager. For example, to view a Logical_Interface_Controller record, choose **Logical Interface Controller** from the Requesters menu. The Configuration Manager displays a list of records. To view a specific record, double-click on it, or select it and click the **Update** button.

To complete the installation of PGs, you need to get a few specific values from the records you create in the Configuration Manager, namely, the Logical Controller ID from the Logical_Interface_Controller record and the Peripheral ID from each Peripheral record.

How to Enable Device Management Protocol Connections

If you have not already done so, you must enable Device Management Protocol (DMP) connections within the CallRouter for each PG.

Step 1 Run the local version of ICM Setup that was installed on the CallRouter machine. (The executable is ICMSetup.exe in the \icm\bin directory.)

Step 2 In the ICM Instance section of the Cisco ICM Setup dialog box, select the desired instance.

Step 3 In the Instance Components section of the Cisco ICM Setup dialog box, select the Router and click Edit.

Step 4 Proceed to the CallRouter's Device Management Protocol Properties dialog box, as described in Chapter 2, "CallRouter Setup". Then make appropriate entries as discussed in "How to Set Device Management Protocol Properties".

See Also

Cisco ICM Setup dialog box (page 19). For setting DMP properties, How to Set Device Management Protocol Properties (page 27).

How to Install a Peripheral Gateway

How to Add a Peripheral Gateway Component

Step 1 In the Cisco ICM Setup dialog box, in the left column under ICM Instances, select an instance.

Step 2 Click **Add** in the Instance Components section.

The ICM Component Selection dialog box opens.

Step 3 Click **Peripheral Gateway**.

The Peripheral Gateway Properties dialog box opens.

See Also

Cisco ICM Setup dialog box (page 19); ICM Component Selection dialog box (page 24).

How to Set Peripheral Gateway Properties

Step 1 In the Peripheral Gateway Properties dialog box, check **Production mode** and **Auto start at system startup** unless you are specifically told otherwise by your ICM support provider. This ensures that the Peripheral Gateway can restart itself automatically if necessary.

Note:

- However, set the Auto Start feature only **after** your ICM installation is otherwise complete. The server may need to be rebooted a number of times during installation, and problems could occur if the node starts before patches and/or databases are applied.
- The **IPCC Express Gateway** PG may not be set to Auto Start; it must be started manually. If Auto Start is selected for this PG, it will have no effect.

Step 2 Check **Duplexed Peripheral Gateway** if the PG is part of a duplexed pair

Note: The **IPCC Express Gateway** PG can only be installed Simplexed. This PG will be installed as Simplexed Side A even if other selections are made.

Step 3 In the **ID** field, select from the drop-down list the PG's device identifier as enabled in the CallRouter's Device Management Protocol Properties dialog box.

Note: Each logical PG must have a unique device assignment at the CallRouter. (If a PG is duplexed, both physical machines use the same device assignment.) To add another logical PG, you must enable another PG device for the CallRouter.

Step 4 If the PG is duplexed, specify whether you are installing **Side A** or **Side B**. If the PG is simplexed, select Side A.

Step 5 Use the **Client Type Selection** section of the screen to select the type of Peripheral Gateway you want to add. Use the **Add** and **Remove** buttons to select or de-select PG types. You can install one "switch" PG type and one VRU PG at the same time.

Warning: If you select IPCC System as your "switch" PG type, you must also select VRU.

Note:

- If you select **IPCC Enterprise Gateway** or **IPCC Express Gateway** as your "switch" PG type, you cannot also select VRU. If you attempt to add a VRU in this case, an error message is displayed.
- To allow the ICM software to route e-mail if there is no CallManager or ACD PG installed, you need to install and configure both a MediaRouting PG and a NonVoiceAgent PG. CTI Sever must also be configured on both PG machines. The MR PG interface provides routing instructions to the Cisco E-Mail Manager application, while the Non-Voice Agent PG configuration is used to report agent state and status to the ICM software.

Step 6 Choose the local **Drive** on which you want to install the PG software.

Note: Be sure to note the drive you are using for future reference, since this information is required when applying software patches.

Step 7 Choose the **Language** from the list.

Step 8 Click **Next**.

The Peripheral Gateway Component Properties dialog box opens.

See Also

For the CallRouter's Device Management Protocol Properties dialog box, How to Enable Device Management Protocol Connections (page 60).

How to Set Peripheral Gateway Component Properties

Step 1 In the Peripheral Gateway Component Properties dialog box, in the Peripheral Interface Managers section, click **Add**.

The Add PIM dialog box opens.

Step 2 After you are done adding PIMs, in the Peripheral Gateway Configuration section, enter the **Logical controller ID** from the Logical_Interface_Controller record for the PG. You can view the Logical_Interface_Controller record for the PG using the PG Explorer tool from the Configuration Manager.

Step 3 The **CTI Call Wrapup Data Delay** applies only if a CTI application interfaces with the PG. The option specifies the number of seconds the PG waits for the CTI client to send data after the agent finishes call wrap-up. The default is 120 seconds. The PG waits this long for the CTI client to explicitly release the wrap-up data. If the time expires, the PG assumes the wrap-up data are complete.

Each of the remaining options in this dialog box is available only for specific peripheral types.

Step 4 The **Demand command server** option is enabled only if the PG supports Galaxy ACDs. Check this option if you want to use the ICM's Demand Command Client to send demand commands to the ACD.

Step 5 The **Event Link** option is available only if the PG supports Aspect CallCenter ACDs. Check this option if you want the PG to communicate with the ACD through the Aspect Event Link.

Step 6 The **MIS Enabled** option is available only if the PG supports Managed Interface Service. Check this option if you want the PG to the peripheral's MIS subsystem.

Step 7 The **VRU Reporting** section and its options are available only if the PG supports VRUs—and if the default behavior for VRU reporting is not enforced. Select the option that you want to use for VRU reporting. The **Service Control** option is enabled by default.

Step 8 The **Definity ECS Setting** section and its options are available only if the PG supports Avaya DEFINITY ECS ACDs. Check the appropriate option to specify whether the ACD runs in **non-EAS** mode, normal **EAS** mode, or **EAS** with **PHD** mode. The **Using MAPD** option is for DEFINITY ACDs which use the MAP/D interface.

Step 9 When you click the **Advanced** button in the Peripheral Gateway Component Properties dialog box, the MDS and DMP Properties dialog box opens.

Step 10 When you are done setting options in the Peripheral Gateway Component Properties dialog box, click **Next**.

The Device Management Protocol Properties dialog box appears.

See Also

For the Add PIM dialog box, How to Add Peripheral Interface Managers (page 68). For the the MDS and DMP Properties dialog box, How to Set MDS and DMP Properties (page 64). For the Device Management Protocol Properties dialog box, How to Set Device Management Protocol Properties (page 64).

How to Set MDS and DMP Properties

Step 1 In the MDS & DMP Properties dialog box, in the Message Delivery System section, do not change the default values for the **Timed delivery queue interval** or the **Timed deliver queue threshold**, unless told to do so by your ICM support provider.

Step 2 The **Disable ICM time synchronization** option is used to select time synchronization service. The box is checked, by default, since the Windows operating system uses its own integrated time service. However, if the machine is a workgroup machine, uncheck this box to enable ICM Time Synchronization. Note that Setup will not change current configuration when performing an Upgrade all.

Step 3 In the Device Management Protocol section, for the **ICM system ID**, enter the number of the PG as specified in the Peripheral Gateway Properties window (for example, enter 3 for PG 3).

The **Network Probe interval** determines how frequently the PG sends test messages to the CallRouter. Do not change this value unless told to do so by your ICM support provider.

Step 4 Click **OK** when you are finished with this dialog box.

This accepts the information that you entered, and returns you to the Peripheral Gateway Component Properties dialog box.

See Also

For the Peripheral Gateway Component Properties dialog box, How to Set Peripheral Gateway Component Properties (page 63).

How to Set Device Management Protocol Properties

When you click **Next** in the Peripheral Gateway Component Properties dialog box, the Device Management Protocol Properties dialog box opens.

Step 1 In the Device Management Protocol Properties dialog box, 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.

Step 2 Indicate, for both Side A and Side B (if duplexed), whether the PG is local to (**CallRouter is local**) or remote from (**CallRouter is remote (WAN)**) each side of the Central Controller.

Step 3 The **Usable bandwidth (Kbps)** fields input the bandwidth (in kilobits per second) available from the PG to the CallRouter, side A and side B.

a. If the CallRouter is local, the default is 30000 Kbps. This is usually an appropriate value.

b. If the CallRouter is remote, the default is 320 Kbps. This is usually an appropriate value.

Step 4 In the **Heartbeat interval (100 ms)** fields, the default value of 4 (that is, 400 milliseconds) is usually appropriate.

Heartbeats from a remote PG to the CallRouter must compete with other network traffic on the visible WAN. If bandwidth is limited, you might want to reduce the frequency of these heartbeats to allow for the timely delivery of other data from the PG. On the other hand, if the heartbeat interval is too long, network error bursts might interfere with heartbeat detection. This can cause the CallRouter to send unnecessary diagnostic traffic which places a further load on the network.

Step 5 Click **Next**.

The Peripheral Gateway Network Interfaces dialog box opens.

See Also

For the Peripheral Gateway Component Properties dialog box, How to Set Peripheral Gateway Component Properties (page 63)

How to Set Peripheral Gateway Network Interfaces

Step 1 In the Peripheral Gateway Network Interfaces dialog box, in the Private Interfaces section, enter the TCP/IP addresses of the private network for the PG machines (**PG private A**, **PG private A high**) and, if it is duplexed, its pair (**PG private B**, **PG private B high**). If the PG is simplexed, enter **localhost** for the B side addresses.

Step 2 In the Visible Interfaces section, enter the visible network addresses for the PG (**PG visible A**, **PG visible B**)and CallRouter (**Router visible A**, **Router visible A high**, **Router visible B**, **Router visible B high**) machines—see How to Set Central Controller Network Interfaces. If simplexed, enter **localhost** for the B side addresses.

Step 3 If you wish to use the Cisco ICM Quality of Service (QoS) feature for the Private Interfaces, click **QoS...** in that section.

The PG Private Link QoS Settings dialog box opens.

Step 4 If you wish to use the Cisco ICM Quality of Service (QoS) feature for the Visible Interfaces, click **QoS...** in that section.

The PG Visible Link QoS Settings dialog box opens.

Step 5 If you do not wish to use QoS—or after you have made your QoS settings—click **Next**.

The Check Setup Information window opens.

See Also

For Router interfaces, How to Set Central Controller Network Interfaces (page 28). For the PG Private Link QoS Settings dialog box, How to Set the QoS Feature for the PG Private Interfaces (page 66). For the PG Visible Link QoS Settings dialog box, How to Set the QoS Feature for the PG Visible Interfaces (page 67). For the Check Setup Information window, How to Complete Peripheral Gateway Setup (page 68).

How to Set the QoS Feature for the PG Private Interfaces

The PG Private Link QoS Settings dialog box comes in two forms.

- If you are installing the PG on Side A of a duplexed system, or you are installing the PG on a simplexed system, you see the PG Private Link QoS Settings (Side A) dialog box.
- If you are installing the PG on Side B of a duplexed system, you see the PG Private Link QoS Settings (Side B) dialog box.

Further, the precise nature of the Side A and Side B forms depends on whether you use Microsoft Packet Scheduler or not; that is, there are actually four forms.

Step 1 In the PG Private Link QoS Settings (Side A) dialog box, check **Enable QoS**. (There is no **Enable QoS** box in the PG Private Link QoS Settings (Side B) dialog box. QoS is enabled on Side B if, and only if, it is enabled on Side A.)

Step 2 Check **Use Packet Scheduler** if you plan to use Microsoft Packet Scheduler.

Leave **Use Packet Scheduler** unchecked if you do not plan to use Microsoft Packet Scheduler.

If **Use Packet Scheduler** is checked for Side A, it must be checked for Side B.

If **Use Packet Scheduler** is unchecked for Side A, it must be unchecked for Side B.

Note: Cisco recommends NOT implementing Microsoft Packet Scheduler for ICM 7.0(0). For more information about ICM QoS, and about this recommendation in particular, refer to the *Pre-Installation Planning Guide for Cisco ICM Enterprise Edition*. If you plan to use Microsoft Packet Scheduler you must install it separately—it is not installed from ICM Setup.

Step 3 Select DSCP priority markings and 802.1p priority tagging, and enter Bandwidth information, as appropriate and allowed—if Packet Scheduler is used, Setup checks that **Total usable bandwidth (Kbps)** is at least 1544 and that the **Bandwidth Percent** values add up to 100.

Note the following differences among the four forms:

- With Packet Scheduler there are only two priority levels (High and Low)—the Medium Priority traffic is marked the same as the Low Priority traffic.
- Bandwidth settings are not enabled on Side B because that information is obtained from Side A.
- The Select Network Interface Card list is used only with Packet Scheduler, in which case a Card must be selected from the display of available Cards.
- When using Packet Scheduler, the same DSCP and 802.1p settings must be used for every ICM instance that uses a given Network Interface Card. Record the settings you use to make sure that this rule is followed.
- When not using Packet Scheduler, the Side B dialog box has no fields enabled because that information is obtained from Side A.

Step 4 Click OK, which accepts the information that you entered, and returns you to the Peripheral Gateway Network Interfaces dialog box.

See Also

For the Peripheral Gateway Network Interfaces dialog box, How to Set Peripheral Gateway Network Interfaces (page 65).

How to Set the QoS Feature for the PG Visible Interfaces

Step 1 In the PG Visible Link QoS Settings dialog box, check Use Packet Scheduler if you plan to use Microsoft Packet Scheduler.

Leave **Use Packet Scheduler** unchecked if you do not plan to use Microsoft Packet Scheduler.

Step 2 Select DSCP priority markings and 802.1p priority tagging, and enter Bandwidth information, as appropriate and allowed—if Packet Scheduler is used, Setup checks that **Total Usable Bandwidth (kbps)** for Side A and Side B is at least 56 each and that the **Bandwidth Percent** values add up to 100.

With Packet Scheduler there are only two priority levels (High and Low)—the Medium Priority traffic is marked the same as the High Priority traffic.

Step 3 Click **OK**, which accepts the information that you entered, and returns you to the Peripheral Gateway Network Interfaces dialog box.

See Also

For the Peripheral Gateway Network Interfaces dialog box, How to Set Peripheral Gateway Network Interfaces (page 65).

How to Complete Peripheral Gateway Setup

Step 1 In the Check Setup Information window, ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the **Back** button.

Step 2 When the settings are correct, click **Next** to begin copying files.

The copying process may take several minutes to complete. You can continue with other work while Setup operates in the background.

Step 3 If Setup successfully copies all the files, it displays the final screen and asks whether you want to start the ICM Node Manager now. Do not start the Node Manager until you have completed the entire ICM installation.

Step 4 Click **Finish** to exit Setup (and optionally start the Node Manager).

If you choose to start it, the Node Manager automatically starts the other ICM processes on the PG.

After installing the PG software for an Aspect ACD, you might also have to install an Application Bridge Server.

After installing the PG software for a DMS-100 ACD, you might also have to install a CompuCALL Server Gateway.

See Also

For installing an Aspect Application Bridge Server, How to Install an Aspect Application Bridge Server (page 86). For installing a DMS-100 CompuCALL Server Gateway, How to Install a DMS-100 CompuCALL Server Gateway (page 88).

How to Add Peripheral Interface Managers

A Peripheral Interface Manager (PIM) is that part of the PG software that communicates directly with a peripheral. You must add a PIM for each peripheral associated with the PG. Each PG can have up to 32 associated peripherals (and, hence, up to 32 PIMs).

Step 1 In the Add PIM dialog box, select the appropriate **Client Type** from the drop-down list (either the "switch" PG type that was selected in the Peripheral Gateway Properties dialog box, or VRU, if that was selected as well, or instead).

Step 2 Select the PIM to add from the **Available PIMs** list. The list contains only PIM numbers that are not already defined for this PG.

When you click **OK**, a Configuration dialog box appears in which you can enter the properties of the peripheral. In general, the fields in the dialog box are different for each switch type. However, each Configuration dialog box does contain an **Enabled** option, a **Peripheral name** field, and a **Peripheral ID** field.

Click **OK** when you are finished with the Configuration dialog box. This accepts the information that you entered, and returns you to the Peripheral Gateway Component Properties dialog box.

The specific Configuration dialog boxes are described in the following subsections.

See Also

For the Peripheral Gateway Component Properties dialog box, How to Set Peripheral Component Gateway Properties (page 63).

How to Configure the ACP1000 PIM

Step 1 In the ACP1000 Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 In the Supervisor Interface section, enter the **TTY Link Port Number**. The ACP1000 PIM uses this link to obtain agent configuration information when the PIM starts up.

Step 5 In the ApplicationLink Interface section, select the type of interface you want to establish between the PG and the host server.

The choices are:

- **TCP**. Click this radio button if you want to configure an ethernet connection to the host server. Enter the **Host Name** of the server and the TCP **Port Number**.
- **Named Pipe**. Click this radio button if you want to configure a named pipe connection to the host server. Enter the **Pipe Name**.

How to Configure the Alcatel A4400 PIM

Step 1 In the Alcatel A4400 Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 In the **Alcatel host name** field, enter the TCP host name of the Alcatel A4400 system.

Step 5 Optionally, in the **Alcatel backup host name** field, enter the TCP host name of the backup Alcatel A4400 system.

Step 6 In the **Alcatel connection port** field, enter the TCP port number of the Alcatel A4400 system.

Step 7 For Alcatel switch releases 3.0 and greater, you need to check the box labeled **No Events for Calls In Progress**.

How to Configure the Aspect PIM (using Event Link)

The dialog box you see for Aspect ACDs depends on whether or not you chose **Event Link** in the Peripheral Gateway Component Properties dialog box.

If you chose **Event Link**, the Aspect Event Link Configuration dialog box opens:

Step 1 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 Specify the primary and backup CallCenter ACDs for the Aspect Real-Time Bridge (RTB), Application Bridge (AB), and Event Monitor Request (EMR) link.

Step 5 Specify the TCP port used for the Event Monitor Request link in the **Datalink port** field.

Step 6 Also, if you are using the private PG interface, specify that interface in the **Host Interface** field. Otherwise the PG uses the public interface by default. The public and private PG interfaces are IP addresses, or names associated with the IP addresses, defined in the HOSTS file.

Note: After you finish installing the PG, you may wish to install the Aspect Application Bridge Server.

See Also

For the Peripheral Gateway Component Properties dialog box, How to Set Peripheral Gateway Component Properties (page 63). For installing an Aspect Application Bridge Server, How to Install an Aspect Application Bridge Server (page 86).

How to Configure the Aspect PIM (not using Event Link)

The dialog box you see for Aspect ACDs depends on whether or not you chose **Event Link** in the Peripheral Gateway Component Properties dialog box.

If you did not choose **Event Link**, the Aspect Configuration dialog box opens:

Step 1 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 To provide full functionality, the PIM must establish a connection to the Aspect Application Bridge. Enter the port number for this connection (from the Aspect Data Link configuration table) in the **App port** field.

Step 5 Do not check the **Offered by service** option unless your ICM support provider tells you otherwise. This option prevents the PIM from gathering statistics about individual ICM routes.

Note: After you finish installing the PG, you may wish to install the Aspect Application Bridge Server.

See Also

For the Peripheral Gateway Component Properties dialog box, How to Set Peripheral Gateway Component Properties (page 63). For installing an Aspect Application Bridge Server, How to Install an Aspect Application Bridge Server (page 86).

How to Configure the Avaya DEFINITY PIM (not using MAPD)

The dialog box you see for DEFINITY ACDs depends on whether or not you chose the **Using MAPD** option in the Peripheral Gateway Component Properties dialog box.

If you did not choose the **Using MAPD** option, the Definity ECS PIM Configuration (CVLAN on Definity LAN Gateway or BRI CallVisor PC) dialog box opens:

Step 1 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 Check **CMS Enabled** if you plan to use CMS, then fill in the information about the CMS connection in the **Call Management System (CMS) Configuration** section. The **CMS Data Timeout** is in milliseconds.

Step 5 In the **CVLAN Configuration on DLG/BRI CallVisor PC** section, enter the requested information about the CallVisor setup for both sides of a duplexed PG (or only for Side A if simplexed). In the **Minimum number of overall ASAI links before Failover field**, enter the minimum number of Adjunct Switch Application Interface (ASAI) links needed to handle the expected call load. (Each ASAI link can handle up to 8000 busy hour calls.) For each CallVisor host, enter the Hostname, and indicate which ASAI links to use. (Each ASAI link connects to a BRI or Ethernet port on the DEFINITY.)

See Also

For the Peripheral Gateway Component Properties dialog box, How to Set Peripheral Gateway Component Properties (page 63).

How to Configure the Avaya DEFINITY PIM (using MAPD)

The dialog box you see for DEFINITY ACDs depends on whether or not you chose the **Using MAPD** option in the Peripheral Gateway Component Properties dialog box.

If you chose the **Using MAPD** option, the Definity ECS PIM Configuration (CVLAN on MAPD) dialog box opens:

Step 1 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 Use the **CVLAN/MAPD Configuration** fields to describe the Multi-Application Platform in Definity (MAP/D) connections for the PG (and its duplexed pair, if any).

Step 5 In the **Monitor ASAI links** field, indicate which ASAI Links in the MAP/D system the PG will use for monitoring calls, stations, and so forth. In the **Post-Route ASAI links** field, indicate which ASAI Links in the MAP/D system the PG will use for ICM Post-Routingpostroute_def. In the **Heartbeat Maintenance** field, indicate which ASAI Links in the MAP/D system the ICM will use for heartbeat maintenance.

Step 6 In the **Minimum number of overall ASAIs links before failover** field, indicate the minimum number of ASAI links required for the expected call load. If the PG is duplexed and the number

of links available to the PG falls below this value, the ICM attempts to switch over to the other PG. Use the **Default Timed ACW value (Seconds)** field to indicate the default after-call-work (ACW) value for agents. A zero in the field indicates that the ICM will get this value from the peripheral monitor table. Values entered in this field apply only to monitored agents.

See Also

For the Peripheral Gateway Component Properties dialog box, How to Set Peripheral Gateway Component Properties (page 63).

How to Configure the CallManager PIM

To configure the CallManager PIM:

Step 1 In the CallManager Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 In the **Agent extension length** field, enter the number of digits in the agent extension. The default is 7; the maximum is 15.

Step 5 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.

Step 6 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.)

Step 7 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.)

How to Configure the DMS-100 PIM

Step 1 In the DMS-100 Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 In the CompuCALL Sessions section, to configure a new CompuCALL session, click **Add**; to modify an existing session, select the session and click **Edit**.

In either case, the DMS100 Session Configuration dialog box opens.

Step 5 In the DMS100 Session Configuration dialog box, enter or edit the **ApplicationID**, an integer that identifies the ICM as the application that is initiating the logon request.

Step 6 Enter or edit the **BusinessGroupID**, an integer that identifies your company. Your Interexchange Carrier defines this ID.

Step 7 Enter or edit the **NetworkNodeID**, an integer identifier that specifies the switch that the ICM will use to communicate. .

This is the switch the host computer connects to via the CompuCALL link. Your Interexchange Carrier defines this ID.

Step 8 Enter or edit the **Password**, which is the same as the BusinessGroupID's password.

Step 9 Enter or edit the **ServiceID**, an integer that identifies the application context to be set for the session (that is, a service profile containing Application Service Options or subsets, as defined by your Interexchange Carrier).

Step 10 Enter or edit the **ServiceVersion**, an integer that specifies the application level or the signaling version that the host application is using (for example, 35 for BCS35).

The **CompuCALL Link IDs** section shows the CompuCALL links defined on the local computer. The CompuCALL link defines how the ICM PG interacts with the DMS-100.

Step 11 Click **OK**.

This accepts the information that you entered, and returns you to the DMS-100 Configuration dialog box.

Step 12 In the DMS-100 Configuration dialog box, in the CompuCALL Links section, to configure a new CompuCALL link, click **Add**; to modify an existing session, select the link and click **Edit**.

In either case, the DMS100 Link Configuration dialog box opens.

Step 13 In the DMS100 Session Configuration dialog box, the X.25 link option is the only one currently available. Enter or edit the **Port Number**, an integer identifier for the X25 card installed on the local computer.

Step 14 Enter or edit the **User Data**, which is four octets of data (each octet ranging from 0 to 255, expressed in hexadecimal).

These data are provided by the Interexchange Carrier as the PROTOCOL subfield.

Step 15 Enter or edit the **Local Address**, the X25 address of the local computer. The system administrator provides this value.

Step 16 Enter or edit the **Remote Address**, the X25 address of the remote switch. The system administrator provides this value.

Step 17 Click **OK**.

This accepts the information that you entered, and returns you to the DMS-100 Configuration dialog box.

Step 18 Enter the TCP Interface **Hostname** (or IP address) and the **TCP Port Number**.

Note: After you finish installing the PG, you may wish to install the DMS-100 CompuCALL Server Gateway.

See Also

For installing the DMS-100 CompuCALL Server Gateway, How to Install a DMS-100 CompuCALL Server Gateway (page 88)

How to Configure the G2 PIM

Step 1 In the G2 Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 In the **Application host name** field, enter the name of the host computer that passes information to the PIM.

Step 5 In the **Receive connection port** field, enter the PG port number on which the PIM receives the information

---

How to Configure the Galaxy PIM

Step 1 In the Galaxy Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 Specify the Galaxy ACD **X.25 port** used for the Foreign Processor Data Link (FPDL). The PIM connects to this port to monitor data from the Galaxy ACD.

Step 5 The ICM collects information from the Galaxy ACD at the end of each logging period. In the **Log period minutes** field, specify the length of the logging period used by the ACD.

Step 6 In the **Daily cutoff minutes** field, specify how many minutes after midnight the first period of each day begins.

Step 7 In addition to the normal database tables for peripheral historical and real-time data, the ICM optionally populates additional tables with unprocessed historical data directly from the Galaxy. This allows you, for example, to run legacy reports on Galaxy data. You can choose to populate any or all of these additional tables by checking the appropriate options in the **Pass through** section.

Step 8 The VarCTI facility is an optional feature of the Galaxy ACD that provides host computing services through a VarCTI server. If the PG connects to the VarCTI server for the ACD, check the **Enabled** box in the VarCTI section. Then enter the **Hostname** or IP address of the VarCTI server, the **Port** on the server that the PG uses, and the **Switch ID**—the identifier for the ACD recognized by the server.

How to Configure the IPCC Enterprise Gateway PIM

Step 1 In the IPCC Enterprise Gateway Configuration dialog box, 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.

Step 2 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).

Step 3 In the **Peripheral ID** field, from the Peripheral record, enter the Peripheral ID value of the *parent server* from the Configuration Manager (use the PG Explorer tool to view the Peripheral ID).

Step 4 In **System PG A name**, enter the hostname or IP address of the Side A *child server*.

Step 5 In **System PG A port**, enter the port on the Side A *child server* (the server port of the CG).

Step 6 If the child system is duplexed, in **System PG B name** and **System PG B port** enter the corresponding information for Side B. If the child system is simplexed, leave these fields blank.

Step 7 In **System PG Peripheral ID**, enter the Peripheral ID of the Side A child peripheral (if the child system is duplexed, the Peripheral ID is the same for Side A and Side B).

How to Configure the IPCC Express Gateway PIM

Step 1 In the IPCC Express Gateway Configuration dialog box, 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.

Step 2 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).

Step 3 In the **Peripheral ID** field, from the Peripheral record, enter the Peripheral ID value of the *parent server* from the Configuration Manager (use the PG Explorer tool to view the Peripheral ID).

Step 4 In the **IPCC Express Host Name** field, enter the hostname or IP address of the *child server*.

Step 5 In the **IPCC Express Host Port** field, enter the port of the *child server*.

How to Configure the IPCC System PIM

Note: An IPCC System PIM must have a VRU PIM associated with it. When a VRU PIM is installed along with the IPCC System PIM, the Peripheral ID for the VRU will automatically be assigned by Setup, and cannot be changed by the user. The valid range for VRU Peripheral IDs is 4500-4999, starting with 4500. However, if VRUs with Peripheral IDs 4500, 4501, and 4502 exist, and then the VRU with Peripheral ID 4501 is deleted, if a new VRU PIM is added, that new VRU PIM will have the Peripheral ID 4501 rather than 4503. That is, the Peripheral IDs are reusable.

Step 1 In the IPCC System Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 In the **Agent extension length** field, enter the number of digits in the agent extension. The default is 7; the maximum is 15.

Step 5 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.

Step 6 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.)

Step 7 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.)

How to Configure the MD110 PIM

Step 1 In the Ericsson MD110 Configuration dialog box, 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.

Step 2 In the **Peripheral** name field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 In the **Application Link Host** field, enter the IP host name or IP address of the machine with the Application Link software.

Step 5 In the **Connection Port** field, enter the TCP server port used by the Application Link machine. The default is 2555.

Step 6 The **Application Link Option** field must be set to 1.

Step 7 The **CCM ODBC DSN** name must be the same name used when configuring the DSN for the Call Center Manager (CCM) connection.

Step 8 The **CCM Machine Name** must be the name of the machine that holds the CCM database.

Step 9 The **CCM User Name** is the name of the user that has access to the CCM machine.

Step 10 The **CCM Password** is the password assigned for the CCM user.

How to Configure the MediaRouting PIM

The MediaRouting Configuration dialog is used to configure the Media Routing interface. This interface allows application software, such as Cisco E-Mail Manager and Cisco Collaboration Server, to access the ICM software task and agent management services for different customer contact media, such as e-mail, fax, Web-collaboration, Internet-chats, and voice.

Note: In most cases, the MediaRouting PG 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 Media Routing PG to monitor state and activity of agents who are non-voice agents. However, this is optional, and not necessary if you already have a MediaRouting PG configured for Voice agents.

Customer contact applications use the MediaRouting interface to request instructions from the ICM software, when they receive a contact request from a customer using one of the media,

such as e-mail, fax, Web-collaboration, Internet-chat or voice. When the ICM software receives a new task request from the application, the 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.

Step 1 In the MediaRouting Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 In **Application Hostname (1)**, enter the host name or the IP address of the application server machine (Collaboration Server or E-Mail Manager). If using the host name, the name must be in the hosts file.

Step 5 In **Application Connection Port (1)**, enter the port number on the application server machine that the PIM will use to communicate with the application.

Note: If you are configuring the PIM for the Cisco ICM E-Mail Manager option, use 1600 for the connection port number. For the Cisco ICM Collaboration Server option, use the default of 2000. This also applies for the application connection port (2).

Step 6 If two applications will interface with the ICM software, in **Application Hostname (2)**, enter the host name or the IP address of the second application server machine (Collaboration Server or E-Mail Manager). If using the host name, the name must be in the hosts file.

Step 7 If two applications will interface with the ICM software, in **Application Connection Port (2)**, enter the port number on the second application server machine that the PIM will use to communicate with the application.

Step 8 In **Heartbeat Interval (seconds)**, specify how often the PG will check its connection to the application server. The default value is usually appropriate.

Step 9 In **Reconnect Interval (seconds)**, specify how often the PG will try to re-establish a lost connection to the application server. The default value is usually appropriate.

How to Configure the Meridian PIM

In the Meridian Configuration dialog box, the **Simulator machine** option is for internal Cisco use only.

Step 1 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 In the **Interface** section, select the interface to be used between the Meridian and the PG. The following table summarizes the interface options.

Note: The Enhanced CTI interface provides additional detail about call handling (such as transfers and conferences), but also requires additional configuration. For help in choosing the best interface, consult your ICM support provider.

Table 8: Meridian to PG Interfaces

Interface	Description
Enhanced CTI using MEI and Meridian Link or SCCS with MLS	Provides enhanced data for CTI applications in addition to normal Pre-Routing, Post-Routing, and monitoring capabilities.
MEI with Meridian Link or SCCS with MLS for Post-Routing only	Provides normal Pre-Routing, Post-Routing, and monitoring capabilities.
MEI with no Meridian Link or SCCS with MLS	Provides normal Pre-Routing and monitoring capabilities.
High Speed Link	Provides limited capabilities; supported for backwards compatibility only.

Step 5 If you choose the enhanced CTI interface, you can also choose what information to save in Termination Call Detail rows. Information from the MEI or High Speed Link includes queuing information such as delay times. Information from the Meridian Link or SCCS with MLS contains information set by a CTI client, such as call variables and wrap-up data. (If you choose both, the ICM software writes two Termination Call Detail rows for each call.)

Step 6 You can specify the type of DNIS matching that the PG applies to the ACD by checking the **Enable partial DNIS matching**, **Partial DNIS matches on last 4 digits**, and **Match any trunk group** options.

The PG must connect to either the ACD's Meridian Event Interface (MEI) of an associated MAX system or to the High Speed Link (HSL).

If you plan to use the HSL interface, you must have selected **High Speed Link** in the Interface section.

If you plan to use MEI, you must have selected one of the three MEI options in the Interface section.

Note that the PG can connect to an MEI proxy server if there is more than one MEI client.

To support Post-Routing, the PG must connect to the ACD's Meridian Link or SCCS with MLS interface. To enable this feature, you must have chosen one of the two Meridian Link options in the Interface section.

Step 7 If the PG communicates with the PG through the Meridian Event Interface (MEI), fill in the fields in the **MEI configuration** section.

a. In the **MEI Server A** field, enter the IP name or address of the MAX system that is running the MEI. (If you use a name, that name must be in the PG's host file.) Similarly for the **MEI Server B** field if the servers are duplexed.

b. In the **MEI Server A** port field, enter the port number used when MEI was configured on the MAX. The preferred port number is 44444. Similarly for the **MEI Server B** port field if the servers are duplexed.

c. Set the **Client ID** to Cisco_ICM (the default).

Step 8 If the PG has a connection to the ACD's Meridian Link or SCCS with MLS, fill in the fields in the **Meridian Link** configuration section.

a. In the **Server name** field, enter the IP name or address of the Meridian Link or SCCS with MLS system. (If you use a name, that name must be in the PG's host file.)

b. In the **Server port** field, enter the well-known port used by the Meridian Link or SCCS with MLS (3000, by default).

c. In the **Link Host Name** field, enter the TCP hostname specified in the Meridian Link's link 1 configuration file.

d. In the **Link Machine Name** field, enter the Meridian 1 Machine name specified in the Meridian Link's link 0 configuration file.

e. In the **Instance Number** field, enter the Meridian 1 customer number for which the PG routes calls.

Step 9 If the PG communicates with the ACD through the High Speed Link (HSL), fill in the fields in the **High speed link configuration** section.

a. To allow the proper initialization of agent state data, set **MAX screen scrape** to 1 and set **MAX port** to the name of the Meridian MAX port.

b. In **MAX ID** and **MAX password**, enter the MAX supervisor ID and password to be used to retrieve the information.

c. In the **HSL port** field, enter the name of the Meridian HSL port to which the PG connects.

Note: After you finish installing the PG, you may wish to install the Cisco MEI Server. This is used in configurations where multiple connections to the MEI are required. The Cisco MEI Server, and its installation, are discussed in the *Cisco ICM Software ACD Supplement for Nortel Meridian*.

How to Configure the NEAX2400 PIM

Step 1 In the NEAX2400 Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 Enter the **Switch IP Address** of the OAI/Infolink interface of the NEC switch. This can be found by using the AIPT command of the NEC IMXMAT utility.

Step 5 The **Port Number Start** and **Port Number End** must be set to the port number of the first port in the 16 port range of ports provided by the NEC switch. This is currently 1024.

How to Configure the NonVoiceAgent PIM

In most cases, the MediaRouting PG 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 Media Routing PG to monitor state and activity of agents who are non-voice agents. However, this is optional, and not necessary if you already have a MediaRouting PG configured for Voice agents.

Step 1 In the NonVoiceAgent Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

How to Configure the Rolm 9005 PIM

Step 1 In the Rolm 9005 Configuration, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 Enter the **Revision** number of the ACD.

Step 5 In the Supervisor Terminal Settings section, enter the login ID (**Supervisor user ID**) and password (**Supervisor Password**) that the PG will use to connect to the ACD's Supervisor terminal port.

Step 6 Enter the number of the **First COM** port on the PG through which the PG communicates with the Supervisor terminal interface and the total number of COM ports (**Num COM Ports**) the PG uses.

Step 7 In the COM Port Setting section, specify the **Idle timeout** and **Wait timeout** values in milliseconds.

Step 8 Specify the **Baud rate** and **Parity** for the COM ports.

How to Configure the Siemens Hicom PIM

Step 1 In the Siemens 9751 Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 In the **CallBridge host name** field, enter the TCP/IP host name for the CallBridge for Workgroups connection on the ACD.

Step 5 In the **CallBridge connection port** field, enter the port number for the connection (1040 by default).

How to Configure the Spectrum PIM

Step 1 In the Spectrum Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name)

Step 3 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).

Step 4 In the **Spectrum Revision** field, enter the revision number of the Spectrum ACD.

Step 5 If you use a group number greater than 255, set **Two Byte Groups** to 1; otherwise, set to 0.

Step 6 In the Supervisor CRT section, enter the login ID (**Supervisor ID**) and password (**Supervisor Password**) that the PG will use to connect to the Spectrum's Supervisor CRT port.

Step 7 Enter the number of the COM port (**CRT port**) on the PG through which the PG communicates with the Supervisor CRT interface and the baud rate (**CRT baud rate**) of that port.

Step 8 In the Transaction Link section, first specify whether to use the **X.25**, **TCP**, or **DualLink** interface.

a. If you choose X.25, enter the number of the **X.25 port** on the PG through which the PG communicates with the Spectrum's Transaction Link.

b. If you choose TCP or DualLink, enter the TCP **Hostname** for the ACD and the **Port number** for the Transaction Link. Note that two Transaction Link ports are needed configured on the two PDI III cards for Duplex PG with DualLink configuration.

How to Configure the Symposium PIM

Step 1 In the Symposium Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Step 4 In the **SCCS Host** field, enter the IP host name or IP address of the Symposium Call Center Server. If using the IP host name, the name must be in the IP hosts file used by the PG.

Step 5 Use the radio button to set the Symposium version number you are using.

Use the Meridian Link Configuration section to configure the link to the Meridian switch.

Step 6 In the **Link Host Name** field, enter the TCP hostname specified in the link 1 configuration file on the Meridian Link system. The default, Lanlink, is usually appropriate.

Step 7 In the **Link Machine** field, enter the Meridian 1 Machine name specified in the link 0 configuration file on the Meridian Link system. The default, SL16, is usually appropriate.

Step 8 In the **Server port** field, enter the well-known port used by the Meridian Link. The default is 3000.

Step 9 In the **Instance Number** field, enter the instance number on the Meridian 1 for which the PG routes calls. The default is 0.

Use the RTD Link Configuration section to configure the Real Time Data link, which is used for agent reporting.

Step 10 In the **Client Login** field, enter the user name that was assigned for RTD requesters on the SCCS. The default is sysadmin.

Step 11 In the **Client Password** field, enter the password for the specified user. The default is nortel.

Use the HDX Link Configuration section to configure the Host Data Exchange link, which is used for Symposium call scripting processing.

Step 12 In the **Client Host Name** field, enter the IP name or IP address for the Symposium PG machine. If using the IP name, the name must be in the IP hosts file used by the PG.

Step 13 In the **Client Provider** field, enter the ID by which the HDX server will identify the Symposium PG. The default is 64206. Normally, the default is used.

Step 14 In the **Client Instance** field, enter the instance string that the Symposium PG sends to the HDX server. The default is Cisco Symposium PIM. Normally, the default is used.

How to Configure the VRU PIM

To configure the VRU PIM, complete the following steps:

Step 1 In the VRU Configuration dialog box, 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.

Step 2 In the **Peripheral name** field, enter the Peripheral name from the Configuration Manager (use the PG Explorer tool to view the Peripheral name).

Step 3 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).

Note: There are cases in which the Peripheral ID for a VRU is automatically assigned by Setup.

Step 4 In the **VRU host name** field, enter the name by which the VRU is known to the network.

Step 5 Enter the number of the **VRU connection port** that the PG connects to.

Step 6 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.

Step 7 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.

How to Install an Aspect Application Bridge Server

For an Aspect ACD, the ICM Peripheral Gateway connects to the Aspect Application Bridge. If another application also requires a connection to the Application Bridge, then you must install the Application Bridge Server (ABS). Install the ABS after you have installed the PG software.

If the PG is duplexed, the ABS can be either simplexed (run on only one of the PG machines) or duplexed (run on each PG machine). Running ABS duplexed allows applications to continue to receive data if one PG node fails.

How to Add an Application Bridge Server Component

Step 1 In the Cisco ICM Setup dialog box, in the left column under ICM Instances, select an instance.

Step 2 Click **Add** in the Instance Components section.

The ICM Component Selection dialog box opens.

Step 3 Click **Application Bridge Server**.

The Application Bridge Server Properties dialog box opens.

See Also

Cisco ICM Setup dialog box (page 19); ICM Component Selection dialog box (page 24).

How to Set Application Bridge Server Properties

Step 1 In the Application Bridge Server Properties dialog box, in the Node Manager Properties section, choose **Production mode** and **Auto start at system startup** unless you are specifically told otherwise by your ICM support provider.

Step 2 In the **Side preference** section, if you are installing duplexed ABS and you prefer that one side run rather than the other, specify the preferred side.

Step 3 In the **Settings** section, specify the maximum number of unsent messages you want the ABS to queue for each application (**Maximum queue depth**).

Step 4 Specify the maximum amount of time (in seconds) you want the ABS to wait for an application to accept a connection (**Application timeout**).

Step 5 If the ABS is duplexed, specify the maximum amount of time (in seconds) you want the ABS to wait for its duplexed peer to establish a connection (**Partner connect**).

Step 6 Click **Next**.

The Application Bridge Server Applications dialog box opens.

How to Manage Application Bridge Server Applications

The Application Bridge Server Applications dialog box lets you activate, deactivate, add, edit, or remove ABS applications.

Step 1 Do one of the following:

a. Click **Add**, to add a new application.

b. Select an application in the **Applications** list and click **Edit**, to make changes regarding that application.

c. Select an application in the **Applications** list and click **Delete**, to remove that application from the list.

Step 2 If you clicked **Add** or **Edit**, the Application Properties dialog box opens.

Step 3 After you are through managing your applications, click **Next**.

Files are copied as needed and the ABS installation completed.

How to Set Application Properties

Step 1 Add or modify the **Name** of the application. The **Field Separator** may be 47 for a slash (/) or 124 for a vertical line (|). Check the **Active** box if you want the application to be active.

Step 2 In the **CallCenter** section, check the **Connect first** box if you want the ABS to connect to the CallCenter ACD before connecting to the application. Specify in the **Hostname** field the IP address or hostname of the ACD, and in the **Port Number** field the port number that connects to the ACD for the application on the PG.

Step 3 In the **Side A** section, specify in the **Hostname** field the application's IP address or hostname and in the **Port Number** field the PG port number that connects to it.

Step 4 If the application is duplexed, in the **Side B** section, for that side, specify in the **Hostname** field the application's IP address or hostname and in the **Port Number** field the PG port number that connects to it.

Step 5 Click **OK**.

This returns you to the Application Bridge Server Applications dialog box.

See Also

For the Application Bridge Server Applications dialog box, How to Manage Application Bridge Server Applications (page 87)

How to Install a DMS-100 CompuCALL Server Gateway

For a DMS-100 ACD, the ICM Peripheral Gateway connects to the DMS-100 CompuCALL interface. If another application also requires a connection to the DMS-100, then you must install the CompuCALL Server (CCS) so that the PG and application can share a session on the DMS-100. Install the CCS after you have installed the PG software.

How to Add a CompuCALL Server Gateway Component

Step 1 In the Cisco ICM Setup dialog box, in the left column under ICM Instances, select an instance.

Step 2 Click **Add** in the Instance Components section.

The ICM Component Selection dialog box opens.

Step 3 Click **CompuCALL Server Gateway**.

The CompuCALL Server Gateway Properties dialog box opens.

See Also

Cisco ICM Setup dialog box (page 19); ICM Component Selection dialog box (page 24).

How to Set CompuCALL Server Gateway Properties

Step 1 In the CompuCALL Server Gateway Properties dialog box, in the Node Manager Properties section, choose **Production mode** and **Auto start at system startup** unless you are specifically told otherwise by your ICM support provider.

Step 2 In the **CCS node properties** section, enter the CCS Gateway **ID** and the **ICM system ID** number for the CCS Node. Since the CCS must be simplexed, **Side A** is the only option. Choose the local **Drive** on which you want to install CCS. Choose the **Language** from the drop-down list.

Step 3 Click **Next**.

The CompuCALL Server Gateway Component Properties dialog box opens.

How to Manage CompuCALL Server Gateway Component Properties

The CompuCALL Server Gateway Component Properties dialog box lets you add, edit, or remove CompuCALL Server configurations.

Step 1 Do one of the following:

a. Click **Add**, to add a new server configuration.

b. Select a server in the **CompuCALL Servers** list and click **Edit**, to make changes regarding that server configuration.

c. Select a server in the **CompuCALL Servers** list and click **Delete**, to remove that server configuration from the list.

Step 2 If you clicked **Add** or **Edit**, the CompuCALL Server Properties dialog box opens.

Step 3 When you are finished with this dialog box, click **Next**.

The Check Setup Information window opens.

See Also

For the CompuCALL Server Properties dialog box, How to Set CompuCALL Server Properties (page 89). For the Check Setup Information window, How to Check Setup Information (page 93)

How to Set CompuCALL Server Properties

Step 1 In the CompuCALL Server Properties dialog box, if you want to the server to accept any session, check the **Accept Any Session** box.

Step 2 In the **CompuCALL Server Interface Parameters** section, enter the parameters required to configure the connection to the CompuCALL Server. It is not necessary to enter the **ServerID**. In the **EMTPort** field, enter the port number that the DMS PIM uses to communicate with the CCS (40429 is the default). In the **TCP Port** field, enter the port number that the third-party application and the DMS PIM will use to communicate with the CCS (2500 is the default).

Step 3 In the **ACD Links** section, you can Add, Edit or Delete an ACD link. When you click the **Add** or **Edit** button, the ACD Link Configuration dialog box opens and allows you to configure an ACD link.

Step 4 In the **CompuCALL Sessions** section, you can Add, Edit or Delete a CompuCALL session. When you click the **Add** or **Edit** button, the Session Configuration dialog box opens and allows you to configure a session.

Step 5 In the **Application X25 Links** section, you can Add, Edit or Delete an X.25 application link. When you click the **Add** or **Edit** button, the Application X25 Link Configuration dialog box opens and allows you to configure an X.25 application link.

Step 6 When you are finished with this dialog box, click **OK**, which returns you to the CompuCALL Server Gateway Component Properties dialog box.

See Also

For the ACD Link Configuration dialog box, How to Configure an ACD Link (page 90). For the Session Configuration dialog box, How to Configure a Session (page 91). For the Application X25 Link Configuration dialog box, How to Configure an Application X.25 Link (page 92). For the CompuCALL Server Gateway Component Properties dialog box, How to Set CompuCALL Server Gateway Properties (page 88).

How to Configure an ACD Link

Use the ACDLink Configuration dialog box to configure the link between the CCS and the DMS-100 ACD.

Step 1 In the **Link ID** field, enter a unique digit between 1 and 8, to correspond with the ACD Link Parameters selected in the Session Configuration dialog box.

Step 2 In the **Link Name** field, enter a unique name for the link of up to 40 ASCII characters.

Step 3 In the **Link Interface Types** section, select either **X.25** or **TCP**.

Step 4 For either link, enter the **Port Number**.

Step 5 For a TCP link the **Host Name** is the DMS-100 ACD TCP well-known port number. For an X.25 link the **Local Address** is not used.

Step 6 When you are finished entering information in the ACDLink Configuration dialog box, click **OK**, which returns you to the CompuCALL Server Properties dialog box.

See Also

For the Session Configuration dialog box, How to Configure a Session (page 91). For the CompuCALL Server Properties dialog box, How to Set CompuCALL Server Properties (page 89).

How to Configure a Session

Step 1 In the Session Configuration dialog box, in the CompuCALL Login Properties section, enter the following information:

a. The **ApplicationID** is an integer that identifies the ICM as the application that is initiating the logon request.

b. The **BusinessGroupID** is an integer that identifies your company. Your Interexchange Carrier defines this ID.

c. The **NetworkNodeID** is an integer identifier that specifies the switch that the ICM will use to communicate. This is the switch the host computer connects to via the CompuCALL link. Your Interexchange Carrier defines this ID.

d. The **Password** corresponds to the BusinessGroupID.

e. The **ServiceID** is an integer that identifies the application context to be set for the session (that is, a service profile containing Application Service Options or subsets, as defined by your Interexchange Carrier).

f. The **ServiceVersion** is an integer that specifies the application level or the signaling version that the host application is using (for example, 35 for BCS35).

g. The **TCPLinkSetName** specifies the linkset parameter for TCP connections.

Step 2 In the **ACD Link Parameters** section, select links that will be used by the session. Use the link numbers that are assigned with the ACDLink Configuration dialog box. Enter the X.25 SVC call parameter configured on the DMS-100 in the **X25 User** field. Enter the X.25 SVC call parameter destination DTE address configured on the DMS-100 in the **X25 Remote** field.

Step 3 In the **AppIDs for Unknown Message** section, select the applications that will receive unknown messages. Unknown messages are those that may be introduced in future versions of the CompuCALL interface. The AppID corresponds to the ID listed in the **CompuCALL Applications** section of this dialog box.

Step 4 In the **Session Parameters** section, the **Delay Activation** and **Delay Logon** are not used. Select **Disable Session** if no lower priority applications are allowed to logon, or allowed to remain logged on, unless the highest priority configured application is logged on. **Force Failover** and **Passive Failover** are not used.

Step 5 In the **CompuCALL Applications** section, you can choose to Add, Edit or Delete an application. When you click on **Add** or **Edit**, the Application Configuration dialog box opens.

Step 6 When you are finished entering information in the Session Configuration dialog box, click **OK**, which returns you to the CompuCALL Server Properties dialog box.

See Also

For the ACD Link Configuration dialog box, How to Configure an ACD Link (page 90). For the Application Configuration dialog box, How to Configure an Application (page 92). For the CompuCALL Server Properties dialog box, How to Set CompuCALL Server Properties (page 89).

How to Configure an Application

Use the Application Configuration dialog box to configure the DMS-100 peripheral interface manager and the third party applications that will run for the session.

Step 1 Enter the **Application Name**.

Step 2 In the **Desired Link Count** field, enter the desired number of active links, which is the desired number for the active application with the highest priority.

Step 3 The **Minimum Link Count** field is not currently used.

Step 4 In the **Priority** field, assign a priority number for the application (lower number indicates higher priority).

Step 5 In the **Proxy Application ID** field, enter the Application ID of the third-party application and the DMS-100 PIM (this is the same as the ServerID in the CompuCALL application logon message).

Step 6 When you are finished, click **OK**, which returns you to the Session Configuration dialog box.

See Also

For the Session Configuration dialog box, How to Configure a Session (page 91).

How to Configure an Application X.25 Link

Use the Application X25 Link Configuration dialog box to configure the link between a third-party application and the CCS.

Step 1 Enter **X25 Link ID**, which corresponds to the labels used in the Application Configuration dialog box.

Step 2 In the **X25 Link Name** field, enter a name for the link.

Step 3 Enter the X.25 Port number in the **X25 Port** field.

Step 4 Enter the X.25 DTE address assigned to the link in the **X25 Local Address** field.

Step 5 When you are finished, click **OK**, which returns you to the CompuCALL Server Properties dialog box.

See Also

For the Application Configuration dialog box, How to Configure an Application (page 92). For the CompuCALL Server Properties dialog box, How to Set CompuCALL Server Properties (page 89).

How to Check Setup Information

Step 1 In the Check Interface Setup window, ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the Back button.

Step 2 When the settings are correct, click **Next** to begin copying the files and complete the installation.

Chapter 7

CTI Server Setup

Before Installing CTI Server

Cisco CTI Server is an optional component that allows an external CTI application to communicate with a Peripheral Gateway. The CTI Server is part of the Cisco CTI product.

Note: Cisco supports installation of CTI Server on the same machine where the Peripheral Gateway software is installed. Installing CTI Sever on a machine separate from the PG may cause network problems including, but not limited to, network disconnects, agents missing calls, and agents forced into Not_Ready.

Before installing CTI Server, you must have installed/set up all the other components of ICM as described in the preceding chapters.

How to Install CTI Server

How to Add a CTI Server Component

Step 1 In the Cisco ICM Setup dialog box, in the left column under ICM Instances, select an instance.

Step 2 Click **Add** in the Instance Components section.

The ICM Component Selection dialog box opens.

Step 3 Click **CTI Server**.

The CTI Server Properties dialog box opens.

See Also

Cisco ICM Setup dialog box (page 19); ICM Component Selection dialog box (page 24).

How to Set CTI Server Properties

Step 1 In the CTI Server Properties dialog box, check **Production mode** and **Auto start at system startup** unless you are specifically told otherwise by your ICM support provider. This ensures that the CallRouter can restart itself automatically if necessary.

Note: However, set the Auto Start feature only **after** your ICM installation is otherwise complete. The server may need to be rebooted a number of times during installation, and problems could occur if the node starts before patches and/or databases are applied.

Step 2 Check the **Duplexed CTI Server** option if you are configuring redundant CTI Server machines.

Step 3 In the CG (CTI Gateway) node properties section, the CG node **ID** must match the PG node ID (for example, CG 1 and PG 1).

Step 4 The **ICM system ID** is the Device Management Protocol (DMP) number of the PG associated with the CTI Gateway. Generally this is the same as the number associated with the CG ID in step 3.

Step 5 If the CTI Server will be duplexed, specify which **Side** you are installing: Side A or Side B. If the CTI Server will be simplexed, choose Side A.

Step 6 Choose the local **Drive** on which you want to install the software.

Note: Be sure to note the drive you are using for future reference, since this information is required when applying software patches.

Step 7 Choose the **Language** from the list.

Step 8 Click **Next**.

Setup loads any current installation settings and then the CTI Server Component Properties dialog box opens.

How to Set CTI Server Component Properties

Step 1 In the CTI Server Component Properties dialog box, Setup automatically generates a **Client Connection Port Number**. You can use this value or change to a standard port number. Clients use this port number to connect to the CTI Server.

If you have multiple nodes running on a single machine, each must use a different port number.

Step 2 If you want to require that an agent be logged into the client before the client receives events from the CTI Server, check the **Agent Login Required for Client Events** box. This prevents clients from accessing data for other agents.

Step 3 Click **Next**.

The CTI Server Network Interface Properties dialog box opens.

How to Set CTI Server Network Interface Properties

Step 1 In the CTI Server Network Interface Properties dialog box, in the **PG private interfaces** section, enter the private network addresses for the PG (or PGs, if duplexed) associated with the CTI Server.

Step 2 In the **CG private interfaces** section, enter the private network addresses of the CTI Server.

Step 3 In the **CG visible interfaces** section, enter the visible network addresses of the CTI Server.

Step 4 Click **Next**.

The Check Setup Information window opens.

How to Complete CTI Server Setup

Step 1 In the Check Setup Information window, ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the **Back** button.

Step 2 When the settings are correct, click **Next** to begin copying files.

The copying process may take several minutes to complete. You can continue with other work while Setup operates in the background.

Step 3 If Setup successfully copies all the files, it displays the final screen and asks whether you want to start the ICM Node Manager now. Do not start the Node Manager until you have completed the entire ICM installation.

Step 4 Click **Finish** to exit Setup (and optionally start the Node Manager).

If you choose to start it, the Node Manager automatically starts the other ICM processes on the CTI Server.

Chapter 8

After the Installation

This chapter provides post-installation information. In particular, information is provided on what the ICM Setup program installs, including directories and their contents, and Windows services.

This section contains the following topics:

Files and Directories

ICM Setup installs most of the ICM files under a directory named ICM. If you install the Admin Workstation software, ICM Setup also creates or updates several other files.

The ICM Directory Structure

The ICM Setup procedure creates a directory named ICM in the root directory of the drive you choose. The ICM directory contains a subdirectory for the customer you created in Setup.

The customer directory contains a subdirectory for each component you installed. The following table lists the directory names for each component.

Table 9: Component Installation Directories

Component	Directory Name
Application Bridge Server	ABS

Component	Directory Name
Admin Workstation	AW
CTI Server	CG1A (for CG 1, side A), CG1B (for CG 1, side B), CG2A (for CG 2, side A), ...
Distributor	DIS
Logger	LA (for side A) or LB (for side B)
Outbound Option Dialer	Dialer
Peripheral Gateway	PG1A (for PG 1, side A), PG1B (for PG 1, side B), PG2A (for PG 2, side A), ...
Router	RA (for side A) or RB (for side B)
WebView	AW, Web

For example, if you install the router software for side A, a directory named RA is created in the customer directory under ICM directory.

The following table describes the contents of each subdirectory under the component directories. Note that not all subdirectories apply to all components.

Table 10: Installation Subdirectories

Directory	Components	Contents
bin	all	ICM executable files. Do not modify these files.
custom	Admin Workstation	WebView templates and custom templates. (These files are only used by WebView, and are installed only if WebView is installed.)
export	Admin Workstation, Logger, Distributor	Initially empty. Files written to the export directory on the Logger are automatically copied to Customer Support.
filters	Logger	Files that determine which events are automatically reported to Cisco. Do not modify these files.
hist	Peripheral Gateway	Used by the PG as temporary storage for historical data.
install	Admin Workstation, Logger, Distributor	Files that are used by ICM Setup during initial installation or subsequent Setup changes.
logfiles	all	Initially empty. ICM processes may write log files to this directory.
snmp	all	SNMP files.

Directory	Components	Contents
ssl	Admin Workstation, WebView	SSL files. (Installed only if WebView, Agent Re-skilling, and/or Internet Script Editor are enabled.)
tomcat	Admin Workstation	Tomcat files. (Installed only if Agent Re-skilling is enabled.)
web	WebView	Most WebView-related files.

Other Admin Workstation Files

In addition to the files and subdirectories under the ICM directory, the ICM installs a few additional files in the main Windows and System directory (as indicated by the environment variables %WINDIR% and %SYSDIR%) on each Admin Workstation.

The value of %WINDIR% is the main Windows directory, for example, C:\WINDOWS. The value of %SYSDIR% is the directory that contains Windows system files, for example, C:\WINDOWS\SYSTEM32. Setup may install or upgrade various runtime files in %SYSDIR%.

Two subdirectories of particular note are:

- %SystemDrive%\CiscoUtils\FirewallConfig (which contains the relevant files, including logs, for Windows Firewall configuration)
- %SystemDrive%\CiscoUtils\SecurityTemplates (which contains the relevant template files, and logs, related to Security Hardening)

Configuration Registry

The ICM software stores its environment information in the configuration registry. The configuration registry is a database repository for information about the computer's configuration. You might want to view this information to help diagnose configuration problems. To view the registry, run the Registry Editor (REGEDIT.EXE or REGEDT32.EXE).

Warning: Do not change data directly within the registry. Changes made here can cause unexpected behavior and might be overwritten during a subsequent reboot or Setup. Instead, run ICM Setup and make the appropriate changes.

Within the HKEY_LOCAL_MACHINE tree, Cisco information is stored under SOFTWARE\Cisco Systems, Inc.\ICM. Within the ICM subtree is a subtree for the customer you created in Setup. Within the customer subtree is a key with the ICM node names installed for the customer on this machine (for example, AW, LoggerA, PG2B, RouterB, CG1A, Distributor). Under that are keys for specific parts of the ICM system. For example, under RealTimeClient on an Admin Workstation you can find information about the real-time distributors, and the names and logon information for the central and local databases. Also,

SOFTWARE\Cisco Systems, Inc.\SecurityTemplates\SetupPrompt is the registry named value that can be set to "off" to prevent prompting for Security Hardening.

The Script Editor and several other ICM tools store information within the HKEY_LOCAL_USER tree. This information is stored in subtrees under SOFTWARE\Cisco Systems, Inc.

See Also

Security Hardening Checkbox (page 17).

Node Manager

As part of the installation process, the ICM installation software automatically sets up Cisco ICM Node Manager—Cisco software that manages the other Cisco processes on the machine. Each component for each customer has its own Node Manager, that is, the Node Manager is installed on every ICM system node.

The installation software allows you to set up the Node Manager to start automatically or manually. To see all the services installed on a machine, run the ICM Service Control tool and check the All checkbox.

You can also view and control services through the Services applet in the Control Panel.

The Node Manager starts either automatically or manually depending on the setting you chose for Auto Start in ICM Setup.

Normally, you need not make any changes to Node Manager. However, if you want to remove a Node Manager, run instsrv.exe from the \icm\bin directory.

To setup the Node Manager service again, run the local version of ICM Setup.

Cisco Admin Workstation Program Group

When you install the ICM Admin Workstation software on a computer, the Cisco Admin Workstation program group is created in the Windows Program Manager. This group contains icons for the programs to be run by Admin Workstation users.

To view information about an item in the group, click on the item and choose Properties from the Program Manager's File menu. The following table lists the properties for each item in the Cisco Admin Workstation group. All the files are in the \icm\bin directory.

The ICM Setup program lets you modify the configuration of the Admin Workstation.

Table 11: Program Item Descriptions

Program	File Name
AW Select	awselect.exe

Program	File Name
Call Tracer	scripted.exe/calltracer
Check Routes	rtcheck.exe
CMS Control (if CMS or Agent Re-skilling is enabled)	cmscontrol.exe
Configuration Manager	Launcher.exe
Domain Manager	domainmanager.exe
Glossary	icmgloss.hlp
Initialize Local Database	AWInit.exe
Lock Admin	lockadmin.exe
Router Log Viewer	rtrlog.exe
Scheduled Target Manager	schtargetman.exe
Schema Help	schema.hlp
Script Editor	scripted.exe
Service Control	servicecontrol.exe
Setup	icmsetup.exe
SSL Encryption Utility	sslutil.exe

Windows Firewall Configuration

If you wish to install Windows Firewall service in a manner consistent with ICM software, after installing Cisco ICM Release 7.0:

1. Open the Command window
2. Change directory to %SYSTEMDRIVE%\CiscoUtils\FirewallConfig
3. Type command: cscript.exe CiscoICMfwConfig.vbe
4. Check %SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig.Log for any errors

Then start ICM services.

Note: Any subsequent installation of a new component will require re-deploying the Windows Firewall Configuration script.

For more information, refer to the *Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.

Moving Forward

After installing ICM software, you can move on to the following tasks:

- Setting up your configuration in the ICM database. Refer to the *ICM Configuration Guide for Cisco ICM Enterprise Edition*.
- Creating routing scripts to specify how calls are routed. Refer to the *ICM Scripting and Media Routing Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.
- Monitoring call center performance. Refer to the *WebView Installation and Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*.
- Designing an administration strategy for the ICM system. Refer to the *ICM Administration Guide for Cisco ICM Enterprise Edition*.

Cisco CTI OS is an optional component that allows an external CTI application to communicate with a Peripheral Gateway.

You can install a CTI OS Server on the same machine as the Peripheral Gateway software or on a separate machine.

For more information on CTI OS, refer to the CTI OS documentation.

Index