Cisco ICM Software Upgrade Migration Guide

ICM 4.6.2 to ICM 5.0(0), and
ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0)
August 2007

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: 408 526-4100

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

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

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

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

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)

Cisco ICM Software Upgrade Migration Guide, Release 6.0(0)
Copyright © 2003-2004 Cisco Systems, Inc. All rights reserved.

CONTENTS

About This Guide ix

- Purpose ix
- Audience ix
- Organization x
- Conventions xii
- Other Publications xii
- Obtaining Documentation xii
  - Cisco.com xiii
  - Documentation CD-ROM xiii
  - Ordering Documentation xiii
  - Documentation Feedback xiv
- Obtaining Technical Assistance xiv
  - Cisco.com xiv
  - Technical Assistance Center xv
    - Cisco TAC Website xvi
    - Cisco TAC Escalation Center xvi
- Obtaining Additional Publications and Information xvii

PART 1 **Common Upgrade Information**

CHAPTER 1 **Introduction** 1-1

CHAPTER 2 **ICR/ICM Upgrade Planning** 2-1

- Upgrade Planning 2-1

Pre-upgrade Testing 2-1
Network Inventory 2-2
Data Backup Plan 2-3
Network Configuration Backup 2-4
Default Routing Plan 2-4
Test Plan 2-4
Schedule of Upgrade Activities 2-5
Definition of Upgrade Steps 2-5
Post-upgrade Test Definition 2-6
Stakeholder Notification 2-6

PART 2 ICM 4.6.2 to ICM 5.0 Upgrade Migration

CHAPTER 3 ICM 4.6.2 to ICM 5.0 Upgrade Introduction 3-1

CHAPTER 4 ICM 4.6.2 to ICM 5.0 Upgrade Planning 4-1

Upgrade planning 4-1
ICM 4.6.2 Baseline 4-1
Hardware recommendations 4-2
Software requirements 4-2
CallRouter 4-2
Logger 4-3
Admin Workstation – Real Time Distributor/WebView Server 4-3
Admin Workstation – Real Time Client 4-3
Peripheral Gateway 4-3
Related publications 4-3

CHAPTER 5 ICM 4.6.2 to ICM 5.0 Common Ground Upgrade Migration 5-1

Common Ground ICM Upgrade Migration Events 5-1

Overview 5-1
4.6.2 to 5.0 ICM System Upgrade Migration Events 5-2
Stop the Central Controller side A and the *Key* AW(s) to be upgraded 5-2
Upgrade the *Key* Admin Workstation(s) 5-3
Upgrade ICM Central Controller side A 5-3
Stopping the non-upgraded Central Controller side B 5-3
Invoking the default routing plan 5-4
Start up the upgraded side A of the Central Controller 5-4
Upgrade ICM Central Controller side B 5-4
Upgrade the remaining Admin Workstation(s) 5-5
Upgrade the Peripheral Gateways 5-5
Upgrade MS SQL Server 5-5
Common Ground Upgrade Migration Activities 5-6
Upgrade activities 5-6
How to ... 5-7
Disable configuration changes 5-7
Pre-upgrade Activities 5-8
Determine the Occupied Space in the Logger/HDS Database 5-9
Perform System Backups 5-10
Disable Configuration Changes 5-10
Back up the ICR/ICM Directory 5-11
Backup the Windows NT Registry 5-11
Backup Custom Templates and Reports 5-12
Stop ICM side A 5-12
Upgrade the side A *Key* Admin Workstation(s) 5-12
Upgrade the ICM side A Central Controller 5-14
Stop ICM side B 5-15
Validate network default routing 5-16
Start ICM side A and the *Key* AW(s) 5-16
Validate ICM side A routing is restored 5-17

Make the Go/No Go decision to upgrade ICM side B 5-17
Upgrade the side B *Key* Admin Workstation(s) 5-18
Upgrade the ICM side B Central Controller 5-19
Start ICM side B 5-20
Upgrade the remaining AWs 5-21
Enable configuration updates 5-22
Run Post-Upgrade tests 5-22
Application test 5-22
System Integrity Tests 5-23
Upgrade the Peripheral Gateways (PGs) 5-24
Upgrade MS SQL (optional) 5-26
Set all ICM Services to Automatic start. 5-26
Notify stakeholders 5-26

CHAPTER 6 **ICM 4.6.2 to ICM 5.0 Technology Refresh Upgrade Migration** 6-1
Technology Refresh Upgrade Migration Events 6-1
Overview 6-1
Upgrading MS SQL Server 6-2
ICM Technology Refresh Upgrade Activities 6-3
CallRouter Technology Refresh upgrade 6-3
Logger Technology Refresh upgrade 6-3
Domain Conversion Tool 6-5
AW Technology Refresh upgrade 6-6
HDS Technology Refresh upgrade 6-7
All other component Technology Refresh upgrades (PG included) 6-9

CHAPTER 7 **ICM 4.6.2 to ICM 5.0 Upgrade SQL Server Installation and Upgrade** 7-1
Overview 7-1
Pre-Upgrade database planning 7-1

Installing MS SQL Server 2000 7-1
Installing SQL Server service packs 7-5
Creating ICM Databases 7-5
Upgrading MS SQL Server 7.0 to MS SQL Server 2000 7-6

PART 3 ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Upgrade Migration

CHAPTER 8 ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Upgrade Introduction 8-1

CHAPTER 9 ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Upgrade Planning 9-1
Upgrade planning 9-1
ICM Baseline 9-2
Hardware recommendations 9-2
Software requirements 9-3
CallRouter 9-3
Logger 9-3
Admin Workstation – Real Time Distributor/WebView Server 9-3
Admin Workstation – Real Time Client 9-4
Peripheral Gateway 9-4
Related publications 9-4

CHAPTER 10 ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Common Ground Upgrade Migration 10-1
Common Ground ICM Upgrade Migration Events 10-1
Introduction 10-1
Common Ground Upgrade Migration Method Overviews 10-2

ICM 4.6.2 System to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) System Common Ground Upgrade Migration Overview **10-2**

ICM 5.0 System to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) System Common Ground Upgrade Migration Overview **10-5**

ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Common Ground Upgrade Migration Tasks **10-8**

Common Ground Upgrade Migration Tasks **10-12**

Common Ground Upgrade Migration Task Overview **10-12**

Common Ground Upgrade Migration Task - Detailed Steps **10-16**

Verify the status of each ICM instance **10-16**

Synchronize the Logger Databases **10-16**

Determine the Occupied Space in the Logger/HDS Database **10-17**

Perform System Backups **10-17**

Disable Configuration Changes **10-18**

Backup the GeoTel (ICM 4.6.2) or Cisco Systems, Inc. (ICM 5.0(0)) Registry **10-18**

Backup Custom Templates and Reports **10-18**

Run Pre-upgrade tests **10-19**

Stop ICM side A **10-21**

Upgrade the side A *Key* Admin Workstation(s) **10-21**

Upgrade the ICM side A Central Controller **10-23**

Stop ICM side B and remaining AWs **10-25**

Validate network default routing **10-25**

Start ICM side A and the *Key* AW **10-25**

Validate ICM side A routing is restored **10-26**

Make the Go/No Go decision to upgrade ICM side B **10-26**

Upgrade the side B *Key* Admin Workstation **10-27**

Upgrade the ICM side B Central Controller **10-28**

Start ICM side B **10-30**

Upgrade the remaining AWs **10-30**

Ensure the Configuration database transfer is complete **10-32**

Enable configuration updates **10-32**
Run Post-Upgrade tests **10-32**
Upgrade the Peripheral Gateways (PGs) **10-33**
Upgrade MS SQL (optional) **10-35**
Set all ICM Services to Automatic start. **10-35**
Notify stakeholders **10-36**
Upgrading Localized ICM 5.0 Installations to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Installations **10-36**

CHAPTER 11 **ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Technology Refresh Upgrade Migration** **11-1**

Technology Refresh Upgrade Migration Events **11-1**
Introduction **11-1**
Technology Refresh Upgrade Migration Method Overviews **11-2**
ICM 4.6.2 System to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) System Technology Refresh Upgrade Migration Overview **11-2**
ICM 5.0 System to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) System Technology Refresh Upgrade Migration Overview **11-4**
ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Technology Refresh Upgrade Migration Tasks **11-6**
ICM Technology Refresh Upgrade Tasks **11-7**
Logger Technology Refresh upgrade **11-7**
Domain Conversion Tool **11-10**
CallRouter Technology Refresh upgrade **11-12**
AW Technology Refresh upgrade **11-12**
HDS Technology Refresh upgrade **11-15**
All other component Technology Refresh upgrades (PG included) **11-17**

CHAPTER 12 **ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) SQL Server Installation and Upgrade** **12-1**

Overview **12-1**

Installing MS SQL Server 2000 12-1
Installing SQL Server service packs 12-5
Creating ICM Databases 12-5
Pre-Upgrade database planning 12-8
Upgrading MS SQL Server 7.0 to MS SQL Server 2000 12-8

APPENDIX A System Integrity Tests A-1

APPENDIX B Post-Migration Application Tests B-1

INDEX

About This Guide

Purpose

This manual provides the information and procedures required to perform the upgrade migration of Cisco Intelligent Contact Routing (ICR) and Cisco Intelligent Contact Management (ICM) systems. It is divided into three sections:

- Section 1 discusses upgrade information common to all upgrade migrations.
- Section 2 discusses and provides the procedures required to upgrade a Cisco Intelligent Contact Management (ICM) 4.6.2 software system to a Cisco Intelligent Contact Management (ICM) 5.0(0) software system.
- Section 3 discusses and provides the procedures required to upgrade either a Cisco Intelligent Contact Management (ICM) 4.6.2 software system or a Cisco Intelligent Contact Management (ICM) 5.0(0) software system to a Cisco ICM/IP Contact Center Enterprise Edition, Release 6.0(0).

Audience

This document is intended for both Customer and Cisco representatives performing a system upgrade. This document assumes you are:

- Familiar with the terms and concepts of the Cisco ICM software
- Trained in Cisco ICM software system administration and troubleshooting

Customer Order Number:

Organization

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

Chapter	Description
Chapter 1, "Introduction"	Provides the purpose of this guide and discusses the upgrade migration methods: • Common Ground • Technology Refresh Lists the components interfacing with Cisco ICM software not covered in this guide
Chapter 2, "ICR/ICM Upgrade Planning"	Discusses common issues to be addressed when planning an ICR/ICM upgrade.
Chapter 3, "ICM 4.6.2 to ICM 5.0 Upgrade Introduction"	Provides an introduction to the ICM 4.6.2 to ICM 5.0 upgrade migration and describes the Common Ground and Technology Refresh upgrade migration methods.
Chapter 4, "ICM 4.6.2 to ICM 5.0 Upgrade Planning"	Discusses upgrade planning; the ICM 4.52 baseline; and the ICM 5.0 hardware and software requirements.
Chapter 5, "ICM 4.6.2 to ICM 5.0 Common Ground Upgrade Migration"	Discusses the ICM 4.6.2 to ICM 5.0 Common Ground upgrade migration path. Discusses the steps required to perform a Common Ground ICM software upgrade.
Chapter 6, "ICM 4.6.2 to ICM 5.0 Technology Refresh Upgrade Migration"	Describes the ICM 4.*6.2* to ICM 5.0 Technology Refresh upgrade migration path. Discusses the steps required to perform a Technology Refresh ICM software upgrade.
Chapter 7, "ICM 4.6.2 to ICM 5.0 Upgrade SQL Server Installation and Upgrade"	Discusses the MS SQL Server 7.0 to MS SQL Server 2000 upgrade and the MS SQL Server 2000 installation.
Chapter 8, "ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Upgrade Introduction"	Discusses common issues to be addressed when planning an ICM 4.*6.2* or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) upgrade.

Chapter	Description
Chapter 9, "ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Upgrade Planning"	Discusses upgrade planning; the ICM 4.*6.2* or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) hardware and software requirements.
Chapter 10, "ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Common Ground Upgrade Migration"	Describes the ICM 4.*6.2* or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Common Ground upgrade migration path. Discusses the steps required to perform a Common Ground ICM software upgrade.
Chapter 11, "ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Technology Refresh Upgrade Migration"	Describes the ICM 4.*6.2* or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Technology Refresh upgrade migration path. Discusses the steps required to perform a Technology Refresh ICM software upgrade.
Chapter 12, "ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) SQL Server Installation and Upgrade"	Discusses the MS SQL Server 7.0 to MS SQL Server 2000 upgrade and the MS SQL Server 2000 installation.
Appendix A, "System Integrity Tests"	Provides the System Integrity Test required for system testing upon completion of the upgrade migration.
Appendix B, "Post-Migration Application Tests"	Provides the Post-Migration Application Tests required for system testing upon completion of the upgrade migration.

Conventions

This manual uses the following conventions:

Format	Example
Boldface type is used for user entries, keys, buttons, and folder and submenu names.	Choose **Script > Call Type Manager**.
Italic type indicates one of the following: • A newly introduced term • For emphasis • A generic syntax item that you must replace with a specific value • A title of a publication	• A *skill group* is a collection of agents who share similar skills. • *Do not* use the numerical naming convention that is used in the predefined templates (for example, **persvc01**). • IF (*condition*, *true-value*, *false-value*) • For more information, see the *Cisco ICM Software Database Schema Handbook*.
An arrow (>) indicates an item from a pull-down menu.	The Save command from the File menu is referenced as **File > Save**.

Other Publications

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

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco web sites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

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

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:

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

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

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card 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.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

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

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

Cisco Systems

PART 1

Common Upgrade Information

Introduction

This document describes the proper procedures for upgrading Cisco Intelligent Contact Routing (ICR) and Cisco Intelligent Contact Management (ICM) software systems. Table 1-1 provides the upgrade migration paths covered in this guide.

Table 1-1 Upgrade Migration Paths

From			To		
ICR/ICM	**Windows OS**	**MS SQL**	**ICM**	**Widows OS**	**MS SQL**
ICR 4.1.5	Windows NT SP6a	SQL 6.5 SP5a	ICM 4.6.2	Windows NT SP6a or Windows 2000 SP3	SQL 7.0 SP3/4
ICM 4.5.1	Windows NT SP6a	SQL 6.5 SP5a	ICM 4.6.2	Windows NT SP6a or Windows 2000 SP3	SQL 7.0 SP3/4
ICM 4.6.2	Windows 2000 SP3	SQL 7.0 SP3/4	ICM 5.0	Windows 2000 SP3	SQL 7.0 SP 3/4 or SQL 2000 SP3

For addition information, refer to the *Software Requirements* section of the appropriate Upgrade Planning chapter of this guide.

There are two methods of upgrade migration, the Common Ground method and the Technology Refresh method (see Table 1-2).

Table 1-2 Upgrade Migration Methods

Method	Description
Common Ground	In place upgrade - involves upgrading on your existing hardware.
Technology Refresh	Involves moving specified data from your existing ICR/ICM production system to new ICM software BOM compliant hardware. It is recommended that the new hardware is Cisco ICM Bill of Material (BOM) compliant. http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/ccbubom.pdf

The upgrade migration of a Cisco ICR/ICM production system involves either upgrading or installing (depending upon the method used) the new ICM software, the MS SQL database software, and the Windows operating system; and creating an Active Directory environment.

When planning your Cisco ICR/ICM system upgrade, it is necessary to include, or consider, addition software that interfaces with the Cisco ICM software. Specific versions of the Cisco ICM software are only compatible with specific versions of the following software:

- IPCC including CallManager and IP IVR
- CTI desktop/client
- Unity
- Personal Assistant
- Auto Attendant
- Recording solutions

ICR/ICM Upgrade Planning

Upgrade Planning

When planning to upgrade your ICR/ICM system, first prepare these items:

- Pre-upgrade Testing
- Network Inventory
- Data Backup Plan
- Network Configuration Backup
- Default Routing Plan
- Test Plan
- Detailed Schedule of Upgrade Activities
- Definition of Upgrade Steps
- Post-upgrade Test Definition
- Stakeholder Notification

Pre-upgrade Testing

At the beginning of the maintainance window create a pre-upgrade test plan to establish the benchmark. This benchmark is used when you run the post-upgrade tests you develop to test your ICM system during the various stages of the upgrade process. The following are examples of typical ICM system pre-upgrade tests:

- Application test

- System Integrity Tests:
  - Process testing
  - Redundancy testing
  - Alarm testing
  - Historical reporting testing
  - WebView reporting testing (option)
  - Internet Script Editor testing (option)

Network Inventory

Technology Refresh upgrade migration planning and execution require you draw a comprehensive and accurate system diagram detailing the Cisco ICR/ICM production system's private and visible networks.

The private network is dedicated for Central Controller node communication and used to establish, maintain, and restore synchronization between Central Controller nodes. The private network must have sufficient bandwidth to simultaneously handle traffic associated with the following:

- Synchronization of sides – side A and side B are synchronized in the event of the failure of one side within a reasonable time
- State transfer – data transfer from active side Router to the recovering side router

The visible network is a Cisco shared network for local node communication and remote node communication with the Central Controller. The visible network must have sufficient bandwidth to support traffic associated with the following:

- Active Directory synchronization
- Logger database recovery
- Heartbeats – messages sent every 100 milliseconds to the CallRouter and the PG to determine if they are "alive" or functioning.
- Report inquiries
- Alternate path by fault tolerant software to distinguish between node failures and network failures.

The ICR/ICM system may also have a dedicated signaling access network. The signaling access network is dedicated to the network interface controller (NIC) and to the ICR/ICM CallRouters.

Data Backup Plan

While you may perform normally scheduled backups of your data, it is recommended you define a plan for backing up and restoring system critical data just prior to commencing an upgrade migration. Refer to Table 2-1 to determine the system critical data you must back up and restore, copy and paste, or export and import (based upon the upgrade migration method selected).

Table 2-1 System Critical Data

System Critical Data	Common Ground Upgrade	Technology Refresh Upgrade
Backup the Logger SQL database(s)	Yes	Yes
Backup the Historical Data Server (HDS) SQL database(s)	Yes	Yes
Backup any custom databases	Yes	Yes
Backup SQL databases on the AW(s)	No	Yes
Export the GeoTel registry key on all production system nodes	Yes	Yes
Copy the *icr* directory on all production system nodes	Yes	Yes
Web View users, backup custom templates and saved reports.	No	Yes

When performing a Common Ground upgrade, it is recommended that, prior to commencing the upgrade migration, you “image” each node your system using commercial imaging software. In the unlikely event of a catastrophic failure during the upgrade process, this allows rapid rollback to the original production system.

Network Configuration Backup

It is recommended you create a bootable image of the systems that includes the operating system and the network configuration. This backup is a good business practice to assure system recovery in case catastrophic conditions occur during the upgrade process.

Default Routing Plan

Document and validate your default network routing plan prior to the upgrade. When you cross over from your old ICR/ICM production system to your new ICM system, you will be down for a period of time until the cross over is complete.

Test Plan

Execute test cases at various stages of the upgrade based on your expectations. We recommend that, as a minimum, you test the following areas:

- Pre-upgrade Application test
- Pre-upgrade System Integrity tests
- CTI functionality (as applicable)
- Configuration tools
- Reporting functionality
- Post-upgrade Application test
- Post-upgrade System Integrity tests

Perform test cases when side A is upgraded and running in non-fault tolerant mode, prior to the upgrade of side B. Perform the test cases again when the ICM system is fully upgraded and running in duplex mode.

In addition, schedule appropriate resources to ensure custom CTI functionality after an upgrade.

For additional information, refer to Post-upgrade Test Definition.

Schedule of Upgrade Activities

Due to the complexity of an ICR/ICM production system, it is recommended you create a detailed schedule of upgrade activities. This allows your Project Manager to maintain the status of each machine upgrade. It also helps to use a chart indicating all of the ICR/ICM nodes to be upgraded and their upgrade status.

Upgrades are usually performed during off-peak hours. Keep in mind that you may require more than one upgrade window. Normally, an initial maintenance window is established to get the ICR/ICM Central Controller and critical (key) AWs upgraded first. The remaining AWs and PGs are then scheduled as early as maintenance windows allow.

Note Ensure your AWs have been upgraded to the same software version before bringing them online.

Definition of Upgrade Steps

The upgrade migration of an ICR/ICM system involves numerous steps. From your initial software load, you must install/upgrade the operating system, the ICM software (and options), the database software, and any required third party software.

Be aware that, for a period of time during the upgrade migration, the ICR/ICM system runs in a non-fault tolerant mode. In addition, network default routing takes place when both sides of the Central Controller are “stopped” during the cross over (see Test Plan, page 2-4).

Testing must take place when the side A Central Controller is upgraded and running. The upgrade team must then come to consensus on the success of the testing and make a “go” or “no go” decision to proceed with upgrading the side B Central Controller.

If critical problems are encountered after upgrading side A, the upgrade team could decide to restore the side A Central Controller to the old/prior release.

Post-upgrade Test Definition

You must create a test plan for the various stages of the upgrade process to test your ICM system. The following are examples of typical ICM system post-upgrade tests:

- Application test
- System Integrity tests:
  - Process testing
  - Redundancy testing
  - Alarm testing
  - Historical reporting testing
  - WebView reporting testing (option)
  - Internet Script Editor testing (option)

Refer to Run Post-Upgrade tests for additional details.

Stakeholder Notification

The following ICR/ICM associated personnel from the following organizations must be notified of all upgrade activities and schedules.

- Cisco Technical Assistance Center (TAC)
- Local Cisco representative
  - Account Manager
  - Partner
  - Support Engineer
- ACD and VRU Vendors
- Customer Operations and Emergency Management Center

Cisco Systems

PART 2

ICM 4.6.2 to ICM 5.0 Upgrade Migration

CHAPTER 3

ICM 4.6.2 to ICM 5.0 Upgrade Introduction

This section describes the proper procedures for upgrading Cisco Intelligent Contact Management (ICM) 4.6.2 systems to ICM 5.0.

The upgrade process may be accomplished using one of two possible methods:

- the ICM 4.6.2 to ICM 5.0 Common Ground Upgrade Migration method

  The Common Ground Upgrade Migration method involves upgrading on your existing hardware.

- the ICM 4.6.2 to ICM 5.0 Technology Refresh Upgrade Migration method

  The Technology Refresh Upgrade Migration method involves moving specified data from your existing ICM production system to new ICM software BOM compliant hardware.

  This method is based on the following:

  - the new hardware is Cisco ICM Bill of Material (BOM) compliant

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

  - the new hardware has MS Windows 2000 SP3 and either MS SQL 7.0 SP3/4 or MS SQL 2000 SP2 installed; and is an Active Directory environment.

Components interfacing with Cisco Intelligent Call Manager software not covered in this document:

- IPCC including Call Manager and IPIVR
- CTI desktop/client

- Unity
- Personal Assistant
- Auto Attendant
- Recording solutions

It is necessary, however, to include or consider these components in the overall planning of your Cisco ICM Software upgrade, as certain versions of ICM are compatible with certain versions of the previously mentioned components.

ICM 4.6.2 to ICM 5.0 Upgrade Planning

Upgrade planning

When planning to upgrade your ICM system, first prepare a:

- Network Inventory
- Data Backup Plan
- Network configuration backup
- Default Routing Plan
- Test Plan
- Detailed Schedule of Upgrade Activities
- Definition of Upgrade Steps
- Post-upgrade Test Definition
- Stakeholder Notification

ICM 4.6.2 Baseline

Prior to upgrading the following baseline is necessary when upgrading from a 4.6.2 ICM system to a 5.0 ICM system:

- Cisco ICM 4.6.2
- Microsoft SQL 7.0 SP3/4
- Microsoft Windows 2000 SP3

Note Refer to the *Cisco ICM Windows 2000 Planning for Release 5.0* and the *Cisco ICM Release 5.0 Staging on Windows 2000* guides.

Note If you are upgrading an IPCC system, refer to the IPCC section of the 5.0 ICM Software *Release Notes* or the 5.0 *Cisco ICM Software: IP Contact Center Administration Guide*.

Hardware recommendations

The ICM system hardware (i.e., hard drive(s), memory, etc.) must meet certain requirements to run ICM software release 5.0.

Hardware specifications play a critical part in the successful operation of an ICM system. All servers should be audited prior to the upgrade to determine if a hardware upgrade is required.

First, review the ICM 5.0 hardware and software specifications. The minimum hardware requirements to upgrade to ICM software version 5.0 is found on the Cisco ICM Bill of Material (BOM) found at:

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

Software requirements

Cisco ICM Software release 5.0 requires the following minimal levels of 3rd party software for each ICM component:

CallRouter

- Win2K Server SP3
- PCAnywhere 10.5

Logger

- Win2K Server SP3
- SQL 7 SP3/SP4 or SQL 2000
- PCAnywhere 10.5

Admin Workstation – Real Time Distributor/WebView Server

- Win2K Server SP3
- SQL 7 SP3/SP4 or SQL 2000 SP2
- PCAnywhere 10.5
- Infomaker 8.0.1 (required for ICM WebView custom reporting)
- ICM WebView 3rd Party Software 5.0

Admin Workstation – Real Time Client

- Win2K Server SP3
- PCAnywhere 10.5
- Infomaker 8.0.1

Peripheral Gateway

- Win2K Server SP3
- PCAnywhere 10.5

Related publications

When planning ICM system upgrades, familiarize yourself with Cisco Intelligent Call Management documentation relative to ICM, IPCC, and Remote Monitoring Suite.

Review and have available the following documents when performing a 4.6.2 to 5.0 ICM system upgrade:

- Cisco ICM Software Documentation Set, ICM Software Version 5.0
- Cisco ICM Software WebView Administrator Guide, ICM Software Version 5.0
- Cisco ICM Software 5.0 Release Notes
- Hot Fix *Read Me* File from 5.0 Software CD

CHAPTER 5

ICM 4.6.2 to ICM 5.0 Common Ground Upgrade Migration

Common Ground ICM Upgrade Migration Events

Overview

The upgrade migration of a 4.2.6 ICM system to a 5.0 ICM system involves numerous steps. From your initial software load, you must upgrade the operating system, the ICM software (and options), the database software, and any required third party software.

Once your 4.x ICR/ICM system version is updated to the required ICM 4.6.2 baseline, you then complete the ICM and the appropriate SQL upgrades to reach the upgrade end point of an upgraded 5.0 ICM system.

The 4.6.2 to 5.0 ICM System Upgrade Migration Events section provides a listing of the events occurring during a common ground ICM system upgrade migration, followed by a brief discussion of each. The actual steps to follow during the upgrade migration are found in Common Ground Upgrade Migration Activities, page 5-6.

4.6.2 to 5.0 ICM System Upgrade Migration Events

When upgrading a 4.6.2 ICM system to a 5.0 ICM system:

1. Stop the Central Controller side A and the Key AW(s) to be upgraded
2. Upgrade the Key Admin Workstation(s)
3. Upgrade ICM Central Controller side A
4. Stopping the non-upgraded Central Controller side B
5. Invoking the default routing plan
6. Start up the upgraded side A of the Central Controller
7. Upgrade ICM Central Controller side B
8. Upgrade the remaining Admin Workstation(s)
9. Upgrade the Peripheral Gateways
10. Upgrade MS SQL Server (if planned)

Note Be aware that when you run ICM *setup.exe*, the automatic conversion of the registry keys (from *Geotel* to *Cisco Systems, Inc.,* and *icr* to *icm*) occurs before you obtain access to the *ICM Setup* dialog.

Stop the Central Controller side A and the *Key* AW(s) to be upgraded

Note Stopping the side A Central Controller (assumed side to be upgraded) puts side B (from a Central Controller prospective) into a simplex condition.

Note The management of domain controllers is critical during the ICM upgrade process. Therefore, it is important to remember not to be in the process of rebooting domain controllers when simultaneously upgrading an ICM node.

The ICM upgrade commences with stopping all ICM services on the side A Central Controller (the side A Logger and the side A Router).

The side B Router requires successful connectivity with greater than 50% of the configured Peripheral Gateways (PGs).

Upgrade the *Key* Admin Workstation(s)

Key Admin Workstations must be upgraded with the first side of the Central Controller to be upgraded. This is so complete testing can be completed prior to upgrading the second side of the Central Controller.

A *Key* AW, from a demographics view, is simply the AW used for system administration located near the Central Controller being upgraded.

Admin Workstations must be at the same version as the Central Controllers in order to work properly. Due to this, once the Central Controller side with the upgraded software is brought online, any AWs left at the older version of software should be shut down to avoid continuously attempting to connect to the upgraded Central Controller. Continuous re-connection attempts are eventually refused, but in the interim cause unnecessary overhead on the Central Controller and the network.

Note No configuration changes are allowed during the upgrade process. Any configuration changes must wait until the upgrade is complete.

Upgrade ICM Central Controller side A

Side A CallRouter and Logger are upgraded to the new level of software. However, upon completion of the upgrades and reboot of machines, the Logger and CallRouter Services are not started. The upgrade steps include setting all ICM services to manual before proceeding with the upgrade.

Stopping the non-upgraded Central Controller side B

Stop Central Controller side B. ICM Central Controllers cannot run in duplex mode unless the software levels on sides A and B are identical. Therefore, side B Central Controller must be stopped before the side A Central Controller is started at the new/upgraded software level.

Note Stopping the side B Central Controller puts side A (from a Central Controller prospective) into a simplex condition.

Invoking the default routing plan

Once all Central Controller services are stopped on side B, the Central Controller is started on side A.

For the period of time when the side B Central Controller is stopping the logger and router services until the time that the side A Central Controller (Logger and Router) services come on line, the Service Provider's default network routing plan is invoked.

Start up the upgraded side A of the Central Controller

The side A CallRouter requires successful connectivity with 50% of the configured PGs for that instance.

Before proceeding with the upgrade of the B side central controller, testing should be completed with side A in a simplex condition. Only upon successful completion of testing should a "*Go*" decision be made to continue with upgrading the B side central controller.

To stop the upgrade at this point, stop the ICM software on the upgraded machines and start ICM on the non-upgraded machines. Once the non-upgraded machines are back on line the upgraded machines can be brought back to their original state using the stored image. If no issues are identified, or if a problem is assessed as "non-critical" to the business, the upgrade continues.

Upgrade ICM Central Controller side B

Only upon successful completion of side A simplex testing should a "*Go*" decision be made to continue with upgrade of the side B Central Controller.

Once the Central Controller has successfully synchronized, testing should be completed in duplex mode.

Upgrade the remaining Admin Workstation(s)

Once the ICM system has been successfully tested, the remaining Admin Workstations may be upgraded and started.

Upgrade the Peripheral Gateways

Peripheral Gateways may run at a release lower than a Central Controller release. Therefore, the Peripheral Gateways do not necessarily have to be upgraded during the same maintenance window as the Central Controllers. However, it is strongly recommended that they be upgraded within the same week as the Central Controllers.

Note When upgrading from ICM 4.6.2 to ICM 5.0, any ICM 4.6.2 Call Manager PGs must be at Hotfix 100 before migrating the CallRouter and/or the Logger to ICM 5.0. If the Call Manager PGs are not at Hotfix 100 and passwords are used, users will not be able to login as their passwords will be different. If no passwords are used there is no issue.

Upgrade MS SQL Server

Note It is recommended all operating system and ICM upgrade steps are completed, the historical data migration is complete, and the system is stable prior to performing a SQL upgrade. Verify completion by looking at the *recovery* log on the Logger and the *replication* log on the HDS.

When using the common ground upgrade migration method, you must have already upgraded to the baseline of SQL Server 7 SP3. From this SQL release you then have three options:

1. Stay at SQL Server 7 SP3.
2. Upgrade SQL Server 7 SP3 to SQL Server 7 SP4.
3. Upgrade SQL 7 SP3/4 to SQL 2000 SP2

Common Ground Upgrade Migration Activities

Upgrade activities

Note For the purposes of this guide, it is assumed that side A is the side to be upgraded first.

Perform the upgrade activities in the order listed. Refer to the How to ... section for the detailed steps for each activity.

1. Review and approve your migration plan (see Upgrade Planning)
2. Complete the Pre-upgrade Activities
   a. Determine the Occupied Space in the Logger/HDS Database
      - How to determine how much space is currently occupied in the Logger/HDS database
   b. Perform System Backups
      - How to backup the AW HDS database if the machine is a Historical Data Server
   c. Disable Configuration Changes
   d. Back up the ICR/ICM Directory
   e. Backup the Windows NT Registry
   f. Backup Custom Templates and Reports
3. Disable configuration changes
4. Stop ICM side A
5. Upgrade the side A Key Admin Workstation(s)
6. Upgrade the ICM side A Central Controller
7. Stop ICM side B
8. Validate network default routing
9. Start ICM side A and the Key AW(s)
10. Validate ICM side A routing is restored

11. Make the Go/No Go decision to upgrade ICM side B
12. Upgrade the side B Key Admin Workstation(s)
13. Upgrade the ICM side B Central Controller
14. Start ICM side B
15. Upgrade the remaining AWs
16. Enable configuration updates
17. Run Post-Upgrade tests
    a. Application test
    b. System Integrity Tests
    – Process testing
    – Redundancy testing
    – Alarm testing
    – Historical reporting testing
    – WebView reporting testing (option)
    – Internet Script Editor testing (option)
18. Upgrade the Peripheral Gateways
19. Upgrade MS SQL Server (optional - refer to Chapter 10, "ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Common Ground Upgrade Migration")
20. Set all ICM Services to Automatic start.
21. Stakeholder Notification

How to ...

Disable configuration changes

Disabling configuration updates is accomplished by setting a registry variable for each side of the CallRouter to disallow any updates (updates are prevented and an error message is returned). A simple utility or batch file can be created to make this easy.

Make the following registry changes on the CallRouter:

```
HKEY_LOCAL_MACHINE\Software\
GeoTel\ICR\<instance name>\RouterA\Router\
CurrentVersion\Configuration\Global\
DBMaintenance = 1.
```

Test to ensure configuration updates are now disabled. When you attempt to save a configuration change you should get the following message:

Failed to update the database. Exclusive access to the router denied because configuration changes are currently disabled in the router registry.

Pre-upgrade Activities

Perform the following pre-upgrade activities:

1. Upgrade you ICR/ICM production system to the ICM 4.6.2 Baseline.
2. Validate the system infrastructure.
   a. Verify the status of each ICR/ICM instance:

      At the command prompt, run **rttest** on each CallRouter by entering:
      rttest /*cust instance name* /node CallRouter*x* /*system hostname*

      Confirm that the entire ICR/ICM network infrastructure is intact and that all PGs can see and be seen by both sides of their respective CallRouter.

      If any ICR/ICM system problems are observed, address them prior to preceding with the upgrade.

   b. Confirm that the Logger databases are no more than 65-70% full (30-35% free space). See Determine the Occupied Space in the Logger/HDS Database.

   c. Confirm that the HDS databases are no more than 50% full (50% free space). See Determine the Occupied Space in the Logger/HDS Database.

   d. Ensure the C: drive has adequate space for operating system expansion, temporary space, and ICM expansion on all the machines.

      Also ensure you have enough disk space where ever you intend to back up your registry and ICR/ICM folder backups, as well as your database backups.
3. Ensure an ICM 4.6.2 CD set is available at each site.

4. Notify the stakeholders of the upgrade schedule.
5. Disable any automatic nightly backups.
6. Make the *Go/No Go* decision.

Note The *Go/No Go* decision is dependent upon the state of the system and the environment.

7. Perform System Backups.
8. Disable Configuration Changes.
9. Back up the ICR/ICM Directory on all servers.
10. Backup the Windows NT Registry on all servers.
11. Backup Custom Templates and Reports (optional).

Note If required, arrange with the appropriate resources to backup and restore custom reports. In addition, schedule the appropriate resources to assess custom CTI functionality after an upgrade.

Determine the Occupied Space in the Logger/HDS Database

How to determine how much space is currently occupied in the Logger/HDS database

Step 1 Select **Start > Run**.

Step 2 In the *Run* dialog type **cmd** and click **OK** (or press **Enter**).

Step 3 At the command prompt type **icrdba** (or **icmdba** for ICM 4.5 or later).

Step 4 Drill down to the Logger/HDS database.

Step 5 Right-click **cust_sideX** and select **Properties**.

Step 6 Ensure the Logger has at least 1 GB of RAM (2 GB preferred).

Step 7 Ensure the DB log is sized to a minimum of 400 MB (500 MB max.)

Step 8 Ensure the tempdb is sized to 100 MB.

Step 9 Increase SQL locks to 200,000. The SQL server service must be recycled in order for this change to take place.

Perform System Backups

The ICR/ICM nodes should not be upgraded until preparations have been made to revert the nodes back to their original version of the ICR/ICM software in the unlikely case of a catastrophic failure during the upgrade migration. It is recommended that each ICR/ICM node be imaged using commercial imaging software.

It is also recommended you backup all MS SQL databases using the SQL backup/restore process. A full SQL backup of the database is recommended

Note It is recommended you have adequate amount of free space on the disk to ensure there is sufficient disk space to export the configuration. Additional space is needed to export the historical data. You can export to a network drive.

How to backup the AW HDS database if the machine is a Historical Data Server

Step 1 Perform a complete SQL backup of the historical database using the SQL backup/restore procedure. This database needs to be restored to its original location if there is any problem with the upgrade.

Step 2 Copy the *awref.ini* file (found in both the *WINNT* and the *icr\bin* into the *c:\icrbackoutxxx* folder. This file is overwritten during the upgrade process. If it is necessary to revert back to the original version of ICR/ICM, be aware that this file must be moved back as well.

Disable Configuration Changes

Disabling configuration updates is accomplished by setting a registry variable for each side of the CallRouter to disallow any updates (updates are prevented and an error message is returned). A simple utility or batch file can be created to make this easy.

Make the following registry changes on the CallRouter:

```
HKEY_LOCAL_MACHINE\Software\
Cisco\ICM\<instance name>\RouterA\Router\
CurrentVersion\Configuration\Global\
DBMaintenance = 1.
```

Test configuration updates are now disabled.

Back up the ICR/ICM Directory

To backup the ICR/ICM directory:

Step 1 Open a command prompt at the root (C:\) directory.

Step 2 Create a directory called *icrbackoutxxx*, where *xxx* stands for the current version of the ICR/ICM software on the machine. To do this, at the command prompt type: **md \icrbackoutxxx** and press **Return**.

For example, if the machine is currently running ICR version 4.1.5, name the directory *icrbackout415*. If the machine is currently running ICM version 4.5.1, name the directory *icmbackout451*.

Step 3 Change to the *icrbackoutxxx* directory by typing: **cd \icrbackoutxxx** and pressing **Return**.

Step 4 Copy the C:\icr directory into the *c:\icrbackoutxxx* directory.

Step 5 At the command line, type: **xcopy c:\icr c:\icrbackoutXXX /e /k**

Step 6 When the command line asks if *c:\icrbackoutxxx\icr* specifies a filename or directory name in the directory structure, type **D** to indicate a directory. The files now copy over. Otherwise, use the standard Windows copy and paste method to copy the files. Performing this step before the upgrade preserves the files needed to run the ICR/ICM platform at the older version if it is necessary to revert back.

Backup the Windows NT Registry

Saving the registry is done automatically when **Upgrade All** is run. However, to perform this manually, do the following:

Step 1 Open a command prompt and type **regedit** or use **Start > Run> regedit**.

Step 2 Select **HKEY_LOCAL_MACHINE\SOFTWARE\GEOTEL**.

Step 3 Click **Registry > Export registry file**

Step 4 Browse the directory to determine where you want to export the registry file to.

Step 5 Enter a **filename** that will be remembered.

Step 6 Click **Save**.

Backup Custom Templates and Reports

Backing up custom templates and reports is optional, but recommended when performing a Common Ground upgrade migration.

Backup custom templates by coping: *icr\instancename\aw\custom*.

Backup saved reports by coping: *icr\instancename\dis\web\userdata*.

Note When upgrading from Web View I (4.1) to Web View II (4.5 or 4.6), the custom templates created using Active Server Pages for Web View I are not supported in Web View II.

Stop ICM side A

Step 1 **Stop** the side A Router, Logger, and AW/HDS (in that specific order) using the local service control. Set all ICM services to **Manual**.

Note Stop all services individually. Do not use the **Stop All** option.

Step 2 On an AW on the still running side of the old production system, use Script Editor to monitor call routing. Confirm that calls are **not** being default routed. If they are **not**, the upgrade of side A can begin.

Upgrade the side A *Key* Admin Workstation(s)

Step 1 Ensure the Distributor services are stopped, then set them to **Manual**.

Step 2 If this is a WebView Server, run **setup.exe** from the *WebView 3rd Party Software CD* to install *Enterprise Agent Server 4.1.1, JDK 1.3.1, Jaguar CTS 4.1.1,* and *New Atlanta ServletExec ISAPI 4.1.1*. Refer to the

Note If you attempt to upgrade prior to performing this step, you get a message indicating which of the applications is missing and requires installation.

Note If you get a *ReadOnly File Detected* dialog, click D**o not display this message again**, then click **Yes**.

Step 3 Run ICM **setup.exe** from the ICM Installation CD.

Step 4 In the *Question* window the following message is displayed:

Setup is about to convert GeoTel registry to Cisco registry and rename icr directory to icm directory. After the conversion, please perform upgrade to all on the icm system. Do you want to continue?

Select **Yes**.

Step 5 Select **Upgrade All**. The *Upgrade all ICM instances* dialog appears.

Step 6 Press **OK** to upgrade all instance components of this system.

Step 7 If you have WebView, a dialog appears asking for the location of WebView Server. Enter the **DB Server machine name** and click **OK**.

Note If you get a *ReadOnly File Detected* dialog, click D**o not display this message again**, then click **Yes**.

Step 8 Reboot as directed.

Note The ICM processes should not be started until after the Central Controller Side A has been upgraded.

Upgrade the ICM side A Central Controller

Step 1 From the Cisco ICM media, run ICM **setup** to first upgrade the side A Router, then the side A Logger. Select **Upgrade All** for each.

Step 2 On the *Question* screen the following message is displayed:

Setup is about to convert GeoTel registry to Cisco registry and rename icr directory to icm directory. After the conversion, please perform upgrade to all on the icm system. Do you want to continue?

Select **Yes**.

Step 3 Select **Upgrade All**. The *Upgrade all ICM instances* dialog appears.

Step 4 Press **OK** to upgrade all instance components of this system.

Caution Do not proceed if the upgrade states that it cannot remove files from the \icm\bin directory.

The files left in the \icm\bin directory are the ones that could not be removed. Typically, this is caused by *rttest.exe* running in the background. To fix this, do the following:

a. Start the *Task Manager* by right-clicking on the task bar and choosing **Task Manager**.

b. Select the **Processes** tab then right click on *rttest.exe* and select **End Task**. Look for multiple instances of this process running in task manager.

c. Once finished, reboot each machine as requested by *setup*. Remember, delay rebooting the Logger until the Router is fully upgraded.

Note If the Restart Windows dialog appears with the message:
Some files could not be updated because they are currently in use by other programs on the system. Files in use will be updated the next time you restart the system.
Select **Yes, I want to restart my computer now**, then **OK**.

Step 5 Apply the necessary Hot Fixes as directed by the Hot Fix *Readme* file.

Step 6 Ensure that the side A machines have returned no errors following the upgrade and the subsequent reboot.

a. Check the log for errors. The **icmsetup.log** file is located in the C:\temp directory. Change to the C:\temp directory and perform the following command line checks.

- Search for errors using: **findstr /i error icmsetup.log**.

Note No response indicates no errors were found.

- Search for failures using: **findstr /i fail icmsetup.log**.

Note No response indicates no failures were found.

- If you wish, review the log in *Notepad* using: **notepad icmsetup.log**.

Stop ICM side B

To stop ICM side B:

Step 1 **Stop** the side B Router, Logger, and AW/HDS (in that specific order) using the local service control. Set all ICM services to **Manual**.

Note Stop all services individually. Do not use the **Stop All** option.

Validate network default routing

To validate network default routing:

Step 1 Refer the local *Service Control* dialog and ensure both the side A and side B Router and Logger services are stopped and set to manual.

Step 2 Validate that *Network Default Routing* is taking place.

Start ICM side A and the *Key* AW(s)

Step 1 Using local service control, start the side A Logger and Router.

Step 2 Once the side A Logger and Router initilization is complete, start the AW/HDS.

Note Start the services individually. Do not use the *Start All* option.

Note After the upgrade, there may be two *ICM Service Control* icons on the desktop. Right-click on each and select **Properties**. Delete the icon having *icr* in the *Target* and *Start in* fields. Use the *ICM Service Control* icon with *icm* in the *Target* and *Start in* fields.

Step 3 Look for the UAW (*UpdateAW.exe*) process running in the desktop taskbar with the line *Nothing to do.* At this point, its configuration should match that of the logger and all the standard tools should be usable.

If this AW is a Real-Time Distributor (RTD), the last line of the RTDist process running in the desktop taskbar should state *Preferred DB restored.*

Validate ICM side A routing is restored

Step 1 Enable configuration updates for all instances by setting the following registry variable in the CallRouter.

```
HKEY_LOCAL_MACHINE\Software\
Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\
CurrentVersion\Configuration\Global\
DBMaintenance = 0.
```

Step 2 Run simplex tests to check:

a. Call routing

b. AW configuration and scripting

c. WebView and Internet Script Editor access by a pre-upgrade and a post-upgrade created user.

When these checks are completed, refer to Make the Go/No Go decision to upgrade ICM side B.

Make the *Go*/*No Go* decision to upgrade ICM side B

If the tests to validate that ICM side A routing is restored are successful and the decision is to proceed (*Go*), then continue to the next section - Upgrade the side B Key Admin Workstation(s).

If tests to validate that ICM side A routing is restored are not successful and the decision is not to go forward (*No Go*) then:

Step 1 Stop ICM side A.

Step 2 Start up ICM side B.

Step 3 Revert ICM side A back to the prior release using the saved image.

Step 4 Restart side A.

Step 5 Enable configuration updates for all instances by setting the registry variable in the CallRouter. The following registry change should be made on the CallRouter:

```
HKEY_LOCAL_MACHINE\Software\
GeoTel\ICR\<instance name>\RouterA\Router\
```

```
CurrentVersion\Configuration\Global\
DBMaintenance = 0.
```

Upgrade the side B *Key* Admin Workstation(s)

Step 1 Disable configuration changes by making the following registry changes on the CallRouter:

```
HKEY_LOCAL_MACHINE\Software\
GeoTel\ICR\<instance name>\RouterA\Router\
CurrentVersion\Configuration\Global\
DBMaintenance = 1.
```

Step 2 Ensure the Distributor services are stopped, then set them to **Manual**.

Step 3 If this is a WebView Server, run **setup.exe** from the *WebView 3rd Party Software CD* to install *Enterprise Agent Server 4.1.1, JDK 1.3.1, Jaguar CTS 4.1.1,* and *New Atlanta ServletExec ISAPI 4.1.1*.

Note If you attempt to upgrade prior to performing this step, you get a message indicating which of the applications is missing and requires installation.

Note If you get a *ReadOnly File Detected* dialog, click D**o not display this message again**, then click **Yes**.

Step 4 Run ICM **setup.exe** from the ICM Installation CD.

Step 5 In the *Question* window the following message is displayed:

Setup is about to convert GeoTel registry to Cisco registry and rename icr directory to icm directory. After the conversion, please perform upgrade to all on the icm system. Do you want to continue?

Select **Yes**.

Step 6 Select **Upgrade All**. The *Upgrade all ICM instances* dialog appears.

Step 7 Press **OK** to upgrade all instance components of this system.

Step 8 If you have WebView, a dialog appears asking for the location of WebView Server. Enter the **DB Server machine name** and click **OK**.

Note If you get a *ReadOnly File Detected* dialog, click D**o not display this message again**, then click **Yes**.

Step 9 Reboot as directed.

Note The ICM processes should not be started until after the Central Controller Side B has been upgraded.

Upgrade the ICM side B Central Controller

Step 1 From the Cisco ICM media, run ICM **setup** to first upgrade the side B Router, then the side B Logger. Select **Upgrade All** for each.

Step 2 On the *Question* screen the following message is displayed:

Setup is about to convert GeoTel registry to Cisco registry and rename icr directory to icm directory. After the conversion, please perform upgrade to all on the icm system. Do you want to continue?

Select **Yes**.

Step 3 Select **Upgrade All**. The *Upgrade all ICM instances* dialog appears.

Step 4 Press **OK** to upgrade all instance components of this system.

Caution Do not proceed if the upgrade states that it cannot remove files from the \icm\bin directory.

The files left in the \icm\bin directory are the ones that could not be removed. Typically, this is caused by *rttest.exe* running in the background. To fix this, do the following:

a. Start the *Task Manager* by right-clicking on the task bar and choosing **Task Manager**.

b. Select the **Processes** tab then right click on *rttest.exe* and select **End Task**. Look for multiple instances of this process running in task manager.

c. Once finished, reboot each machine as requested by *setup*. Remember, delay rebooting the Logger until the Router is fully upgraded.

Note If the Restart Windows dialog appears with the message:
Some files could not be updated because they are currently in use by other programs on the system. Files in use will be updated the next time you restart the system.
Select **Yes, I want to restart my computer now**, then **OK**.

Step 5 Apply the necessary Hot Fixes as directed by the Hot Fix *Readme* file.

Step 6 If Web View is installed, ensure the *web* process has started.

Step 7 Ensure that the side A machines have returned no errors following the upgrade and the subsequent reboot.

a. Check the log for errors. The **icmsetup.log** file is located in the C:\temp directory. Change to the C:\temp directory and perform the following command line checks.

- Search for errors using: **findstr /i error icmsetup.log**.

Note No response indicates no errors were found.

- Search for failures using: **findstr /i fail icmsetup.log**.

Note No response indicates no failures were found.

- If you wish, review the log in *Notepad* using: **notepad icmsetup.log**.

Start ICM side B

Step 1 Using local service control, start the ICM side B services in the following order:

a. Router

b. Logger

c. AW/HDS

Note Start the services individually. Do not use the *Start All* option.

Upgrade the remaining AWs

Step 1 Ensure the Distributor/Client services are stopped, then set them to **Manual**.

Step 2 If this is a WebView Client, run **setup.exe** from the *WebView 3rd Party Software CD* to install *Enterprise Agent Server 4.1.1, JDK 1.3.1, Jaguar CTS 4.1.1,* and *New Atlanta ServletExec ISAPI 4.1.1*.

Note If you attempt to upgrade prior to performing this step, you get a message indicating which of the applications is missing and requires installation.

Note If you get a *ReadOnly File Detected* dialog, click D**o not display this message again**, then click **Yes**.

Step 3 Run ICM **setup.exe** from the ICM Installation CD.

Step 4 In the *Question* window the following message is displayed:

Setup is about to convert GeoTel registry to Cisco registry and rename icr directory to icm directory. After the conversion, please perform upgrade to all on the icm system. Do you want to continue?

Select **Yes**.

Step 5 Select **Upgrade All**. The *Upgrade all ICM instances* dialog appears.

Step 6 Press **OK** to upgrade all instance components of this system.

Step 7 If you have WebView, a dialog appears asking for the location of WebView Server. Enter the **DB Server machine name** and click **OK**.

Note If you get a *ReadOnly File Detected* dialog, click D**o not display this message again**, then click **Yes**.

Step 8 Reboot as directed.

Note The ICM processes should not be started until after the Central Controller Side B has been upgraded.

Enable configuration updates

Step 1 Enable configuration updates for all instances by setting the registry variable in the CallRouter. The following registry change should be made on the CallRouter:

```
HKEY_LOCAL_MACHINE\Software\
Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\
CurrentVersion\Configuration\Global\
DBMaintenance = 0.
```

Step 2 Test that configuration updates have been enabled.

Run Post-Upgrade tests

A test plan is utilized at various stages of the upgrade process. It is up to you to develop the actual test cases with actual dialed numbers, labels, targets, and expected results. The key areas in which to develop test cases follow.

Application test

The most crucial test is the ability of the system to route calls to defined peripheral targets. Side A of the ICM system is upgraded to ICM 5.0 first, then returned to service. Monitor the ICM call routing decisions to determine if it is making the appropriate routing decisions. The Key AWs, upgraded prior to the side B Central Controller, are used to monitor call routing.

System Integrity Tests

The remaining tests are performed to ensure proper functionality of all system components when the ICM is running in duplex mode. Give special attention to redundancy testing.

Process testing

Validate processes on the ICM system. For example, check the following processes for:

RTR - *all configuration data transferred from logger*

LGR - *completed initialization*

AW - *updateAW has completed update and waiting work*

Step 1 Ensure each software process is running according to specification.

Step 2 Check each NIC for the proper connection to the carrier (IXC) network.

Step 3 Halt and restart each process.

Redundancy testing

Step 1 Stop each active PG to ensure that the back-up PG assumes an active state.

Step 2 Stop the active CallRouter side to ensure that the system switches to the alternate CallRouter side without loss of functionality.

Step 3 Perform the same tests on the logger and the NIC.

Alarm testing

Step 1 Verify your Network Operations Center (responsible for Alarm Tracker monitoring of the system) is receiving the alarms in their tracking system.

Historical reporting testing

Step 1 Launch queries against the upgraded Loggers to ensure the presence and integrity of historical call detail.

WebView reporting testing (option)

Step 1 Open the commonly used WebView views.

Step 2 Examine the data presented.

Internet Script Editor testing (option)

Step 1 Open the most commonly monitored ICM scripts using Internet Script Editor.

Step 2 Examine the data presented.

Upgrade the Peripheral Gateways (PGs)

Note If upgrade planning determines there are redundant PGs, ensure the redundant PGs are up and running properly prior to upgrading the primary PGs.

To upgrade the PGs:

Step 1 When the ICM system (the Router, Logger, and AW/HDS) have stabilized, shut down each primary PG as you intend to upgrade it.

Step 2 Run ICM **setup.exe** (from the media) on each primary PG.

Step 3 In the *Question* window the following message is displayed:

Setup is about to convert GeoTel registry to Cisco registry and rename icr directory to icm directory. After the conversion, please perform upgrade to all on the icm system. Do you want to continue?

Step 4 Select **Upgrade All**. The *Upgrade all ICM instances* dialog appears.

Step 5 Press **OK** to upgrade all instance components of this system.

Caution Do not proceed if the upgrade states that it cannot remove files from the \icm\bin directory.

The files left in the \icm\bin directory are the ones that could not be removed. Typically, this is caused by *rttest.exe* running in the background. To fix this, do the following:

a. Start the *Task Manager* by right-clicking on the task bar and choosing **Task Manager**.

b. Select the **Processes** tab then right click on *rttest.exe* and select **End Task**. Look for multiple instances of this process running in task manager.

c. Once finished, reboot each machine as requested by *setup*. Remember, delay rebooting the Logger until the Router is fully upgraded.

Note If the Restart Windows dialog appears with the message:
Some files could not be updated because they are currently in use by other programs on the system. Files in use will be updated the next time you restart the system.
Select **Yes, I want to restart my computer now**, then **OK**.

Step 6 Apply the necessary Hot Fixes as directed by the Hot Fix *Readme* file.

Step 7 Start the PG processes using ICM Service Control.

Step 8 Ensure that the PGs have returned no errors following the upgrade and the subsequent reboot.

a. Check the log for errors. The **icmsetup.log** file is located in the C:\temp directory. Change to the C:\temp directory and perform the following command line checks.

   – Search for errors using: **findstr /i error icmsetup.log**.

Note No response indicates no errors were found.

– Search for failures using: **findstr /i fail icmsetup.log**.

Note No response indicates no failures were found.

– If you wish, review the log in *Notepad* using: **notepad icmsetup.log**.

Upgrade MS SQL (optional)

Refer to Chapter 7, "ICM 4.6.2 to ICM 5.0 Upgrade SQL Server Installation and Upgrade" for details MS SQL upgrade information and detailed steps.

Set all ICM Services to Automatic start.

Step 1 Double-click the local **ICM Service Control** icon on each ICM component.

Step 2 Select each ICM Service and set it to **Automatic start**.

Notify stakeholders

Notify the stakeholders that the upgrade migration is complete (see Stakeholder Notification).

ICM 4.6.2 to ICM 5.0 Technology Refresh Upgrade Migration

Technology Refresh Upgrade Migration Events

Overview

The Technology Refresh method of ICM upgrade migration involves building a new system at the required Cisco ICM 4.6.2 hardware and software levels.

To accomplish this upgrade you must:

- Upgrade the existing production system to the required ICM 4.6.2 Baseline
- Load the new hardware with:
  - SQL7 SP3/4 or SQL 2000 SP2
  - Windows 2000 SP3
  - the 4.6.2 registry
  - custom templates and saved reports
  - the logger database
  - HDS
  - AW DB (if custom templates exist)
  - custom databases
- Install ICM 5.0

- Move users to the new domain

Note No security settings are migrated during the upgrade. Using the domain controller, you must reset the appropriate security settings for migrated ICM users.

The Technology Refresh method is accomplished by loading software on the new machines in the following order:

1. CallRouter (see CallRouter Technology Refresh upgrade)
2. Logger (see Logger Technology Refresh upgrade)
3. Admin Workstation (see AW Technology Refresh upgrade)
4. HDS (see HDS Technology Refresh upgrade)
5. All other components (including PGs) (see All other component Technology Refresh upgrades (PG included))

Upgrading MS SQL Server

Technology Refresh Upgrade Migration Method

Note It is recommended all operating system and ICM upgrade steps are completed, the historical data migration is complete, and the system stable prior to performing a SQL upgrade.

When using the Technology Refresh upgrade migration method, perform a SQL Server 2000 installation, then apply the appropriate service pack (SP2).

ICM Technology Refresh Upgrade Activities

CallRouter Technology Refresh upgrade

How to Technology Refresh upgrade the CallRouter

Step 1 Install Windows 2000 SP3.

Step 2 Join the domain.

Step 3 Export the ICM 4.6.2 registry key tree from the production CallRouter.

Step 4 Import the ICM 4.6.2 registry key tree onto the new CallRouter.

Step 5 Run ICM *setup.exe* on the new CallRouter.

Step 6 **Edit** the **CallRouter** component, making any necessary changes based on the new environment.

Step 7 Exit, then rerun *setup.exe*.

Note While you can use the DNS style domain name (i.e., name.com, name.net) for Active Directory, ICM only supports a NetBIOS name (i.e., name).

Step 8 Run **Upgrade All**.

CallRouter upgrade is complete.

Logger Technology Refresh upgrade

How to Technology Refresh upgrade the Logger

Step 1 Install Windows 2000 SP3.

Step 2 Install Active Directory (on same or separate machine).

Step 3 Set up and configure DNS.

Step 4 Configure a Domain Controller (on same or separate machine).

Step 5 Join the domain.

Step 6 Install MS SQL Server 7.0 SP3/4 or MS SQL Server 2000 SP2.

Step 7 Create a MS SQL Server backup of the production logger database.

Step 8 Restore the MS SQL Server backup onto the new logger using MS SQL backup /restore.

Note Depending upon the version you initially installed, the data file directories are located in a top level directory named either MSSQL or MSSQL7. When restoring the data files, the MS SQL Server Restore function defaults to MSSQL for this directory name. If necessary, manually input the correct path (i.e., MSSQL7) during the Restore function so that it matches the actual directory name.

Step 9 Export the ICM 4.6.2 registry key tree from the production logger.

Step 10 Import the ICM 4.6.2 registry key tree onto the new logger.

Step 11 Run ICM *setup.ex*e on the new logger (from the media, not from local setup).

Step 12 **Edit** the **instance** and insert the ***new domain name***.

Note While you can use the DNS style domain name (i.e., name.com, name.net) for Active Directory, ICM only supports a NetBIOS name (i.e., name).

Step 13 **Edit** the **logger** component, making any necessary changes based on the new environment.

Step 14 Exit, then rerun *setup.exe*.

Step 15 Run **Upgrade All**.

Step 16 Execute the *Domain Conversion Tool* and enter the information for the new environment.

Logger upgrade is complete.

Domain Conversion Tool

The Domain Conversion Tool must be run on both the ICM 4.6.2 and the ICM 5.0 Loggers. Copy the *DomainConversionUtility* from the *ICM Third Party CD* to the root directories of each Logger.

How to run the Domain Conversion Tool for 4.6.2

Step 1 Open a command prompt on the Logger.

Step 2 Change directory to the *DomainConversionUtility* directory then run *domcvt.exe*. For example:

a. At the prompt type: **cd\DomainConversionUtility\domcvt**

b. Press **Enter**. An explanation of the options available for use in the command string appears.

Step 3 Run the Domain Conversion Tool to save user information from the Logger and domain controller into a file you specify. For example:

a. You create the directory *E:\ConversionBackup*.

b. At the prompt type: **domcvt.exe /DB:**<*enter the database name*> **/F:"E:\ConversionBackup\dbname.cvt" /M:E**

Note The location in the command string must be enclosed in double quotes.

c. A log and report is generated and stored in the local *DomainConversionUtility* directory.

Step 4 Verify the file has been created in the location you specified.

How to run the Domain Conversion Tool for 5.0

Note Run the Domain Conversion Tool on the 5.0 Logger after *setup* is complete and the system has been rebooted.

Step 1 Open a command prompt on the Logger.

Step 2 Change directory to the *DomainConversionUtility* directory then run *domcvt.exe*. For example:

a. At the prompt type: **cd\DomainConversionTool\domcvt**

b. Press **Enter**. An explanation of the options available for use in the command string appears.

Step 3 Run the Domain Conversion Tool to move user information from the 4.6.2 Logger and domain controller into the new 5.0 environment. For example:

Note You must be able to access the location of original 4.6.2 file created by the Domain Conversion Tool.

a. Access the directory *E:\ConversionBackup*.

b. At the prompt type:

domcvt.exe /DB:<*enter the database name*> **/F:"E:\ConversionBackup\dbname.cvt" /M:C /OD:**<*enter the old domain name*> ***/ND:***<*enter the new domain name*> ***/P:***<*enter the password*>

Note Using the **/P** switch at the end of the string creates a global password for all users. If you opt not to use a password, do not use the **/P** switch. Be aware, however, this also occurs globally and could constitute a security risk.

Note No user security settings are converted from ICM 4.6.2 to ICM 5.0 during the upgrade migration process. User security settings must be manually input to be re-established for ICM 5.0.

AW Technology Refresh upgrade

How to Technology Refresh upgrade the AW

Step 1 Install Windows 2000 SP3.

Step 2 Join the domain.

Step 3 Install MS SQL Server 7.0 SP3/4 or SQL Server 2000 SP2.

Step 4 If custom templates exist:

a. create a backup of the database

b. restore the 4.6.2 AW DB to the new system using the MS SQL backup/restore process

Step 5 Export the ICM 4.6.2 registry key tree from the production AW.

Step 6 Import the ICM 4.6.2 registry key tree onto the new AW.

Step 7 Run ICM *setup.exe* on the new AW.

Step 8 **Edit** the **AW** component, making any necessary changes based on the new environment (i.e., machine name, domain name).

Note The database location is initially blank. Provide the new database location.

Note While you can use the DNS style domain name (i.e., name.com, name.net) for Active Directory, ICM only supports a NetBIOS name (i.e., name).

Step 9 Exit, then re-run *setup.exe*.

Step 10 Run **Upgrade All**.

AW upgrade is complete.

HDS Technology Refresh upgrade

How to Technology Refresh upgrade the HDS

Step 1 Install Windows 2000 SP3.

Step 2 Join the domain.

Step 3 Install MS SQL Server 7.0 SP3/4 or SQL Server 2000 SP2.

Step 4 Create a MS SQL Server backup of the production HDS database.

Step 5 Restore the MS SQL Server backup onto the new HDS using the MS SQL backup/restore process.

Step 6 Export the appropriate ICM file/folders tree from the production HDS.

Step 7 Import the *icr* file/folders tree onto the new HDS.

- Ensure custom templates, saved reports, and databases are restored:
  - *icr\instancename\aw\custom* for custom templates
  - *icr\instancename\dis\web\userdata* for saved reports

Step 8 Export the *icr* 4.6.2 registry key tree from the production HDS.

Step 9 Import the *icr* 4.6.2 registry key tree onto the new HDS.

Step 10 Run ICM *setup.exe* on the new HDS (from the media, not from local setup).

Step 11 **Edit** the **HDS** component, making any necessary changes based on the new environment.

Note While you can use the DNS style domain name (i.e., name.com, name.net) for Active Directory, ICM only supports a NetBIOS name (i.e., name).

Step 12 Exit, then re-run *setup.exe*.

Step 13 Run **Upgrade All**.

HDS upgrade is complete.

All other component Technology Refresh upgrades (PG included)

How to Technology Refresh upgrade all other components (PG included)

Note When upgrading from ICM 4.6.2 to ICM 5.0, any ICM 4.6.2 Call Manager PGs must be at Hotfix 100 before migrating the CallRouter and/or the Logger to ICM 5.0. If the Call Manager PGs are not at Hotfix 100 and passwords are used, users will not be able to login as their passwords will be different. If no passwords are used there is no issue.

Step 1 Install Windows 2000 SP3.

Step 2 Join the domain.

Step 3 Export the *icr* 4.6.2 registry key tree from the production component.

Step 4 Import the *icr* 4.6.2 registry key tree onto the new component.

Step 5 Run ICM *setup.exe* on the new component.

Step 6 **Edit** the **component**, making any necessary changes based on the new environment.

Note While you can use the DNS style domain name (i.e., name.com, name.net) for Active Directory, ICM only supports a NetBIOS name (i.e., name).

Step 7 Exit, then re-run *setup.ex*e.

Step 8 Run **Upgrade All**.

Other component upgrade migration is complete.

ICM 4.6.2 to ICM 5.0 Upgrade SQL Server Installation and Upgrade

Overview

This topic covers both upgrading SQL Server 7.0 to SQL Server 2000 and installing SQL Server 2000 in the Cisco ICM environment.

Pre-Upgrade database planning

To upgrade from SQL Server 7.0 to SQL Server 2000, there is not much planning to do because there is no data transfer of during the upgrade.

Installing MS SQL Server 2000

SQL Server 2000 can be installed on either Windows NT or Windows 2000 Server. Before running SQL Server 2000 setup, however, some Microsoft fixes have to accomplished, otherwise, the upgrade may fail. Two bugs in the Microsoft knowledge database may cause an error during the SQL 2000 installation

- Q300676 fixes a race condition when running Message.sql.
- Q285100 fixes connectivity problems over the SQL Server Shared Network Library component.

These bug fixes can be downloaded from Microsoft web site. To apply the bug fix, the files on the SQL Server 2000 installation CD have to be copied to a disk. This is because the bug fix requires replacing a few files on the CD. It is not convenient, but Microsoft has confirmed that it is the only way to apply in the bug fix.

Only ICM 5.0 supports SQL Server 2000 and it requires Windows 2000 Server as its running environment to support all ICM 5.0 features.

SQL Server 2000 *Standard Edition* is supported by ICM 5.0.

Refer to How to install SQL Server 2000 and How to create ICM databases for detailed information.

How to install SQL Server 2000

Step 1 Select *SQL Server 2000 Standard Edition* to start SQL Server setup.

Step 2 On the first screen:

a. Select **Install SQL 2000 Server Components**.

b. Select **Install Database Server**.

c. Read the *Welcome* screen.

d. Click **Next**.

Step 3 On the *Computer Name* screen:

a. Choose the default, **Local Computer**.

b. Click **Next**.

Step 4 On the *Installation Selection* screen:

a. Choose the default, **Create a new instance of SQL Server**.

Optionally, install **Client Tools**. (This upgrade option is available only when SQL 7.0 exists on the machine).

b. Click **Next**.

Step 5 On the *User Information* screen:

a. Enter the **user name** and **company name**.

b. Click **Next**.

Step 6 On the *Software License Agreement* screen:

a. Read the terms of the license agreement, then click **Yes**.

Step 7 On the *Installation Definition* screen:

a. Choose the default **Server and Client Tools**.

b. Click **Next**.

Step 8 On the next screen:

a. For Instance Name, check **Default**.

b. Click **Next**.

Step 9 On the *Setup Type* screen (see Figure 2):

a. Select **Custom** for the setup type.

b. Install the program files to any disk with space available (default is C:)

Step 10 On the *Select Components* screen:

a. Uncheck **Install Books Online**.

b. Leave all other fields set to their **default values**.

c. Click **Next**

Step 11 Under *Services Accounts* select items in exactly this order:

a. Customize settings for each service.

b. Select **Use local system account** (SQL Server is already selected).

c. Check **Auto-start service**.

d. Select **SQL Server Agent**.

e. Select **Use local system account**.

f. Check **Auto-start service**.

g. Click **Next**.

Note **Note:** A pop-up dialog explaining a dependency appears, click **OK**.

Step 12 On the *Collation Settings* screen:

a. *S*et *Collation Designer* to **Latin1_General**.

b. Set the *Sort Order* to **Binary**.

c. Leave other files set to their **default values**.

d. Click **Next**.

Step 13 Under *Network Libraries*:

a. Uncheck all choices except for **Named Pips** unless instructed otherwise.

Step 14 On the *Start Copying Files* screen:

a. Read and click **Next**.

Step 15 On the next screen:

a. Select **Per Seat** as the *Licensing method*.

b. Set at least **40 devices** to prevent running out of licenses for database connections.

Note If you need to choose *Processor License* for licensing reasons, make sure there are sufficient concurrent connection licenses so that the system will not run into licensing problems. There should be at least 40 concurrent connections, though the precise number depends on the accessing need.

Step 16 A dialog box with the message *Setup is installing Microsoft Data Accessing Components (MDAC) ...* appears.

Note Occasionally, MDAC installation fails. The remedy is to download MDAC 2.7, or later, from a Microsoft website and install it. Once MDAC has been installed, run SQL Server setup again.

Note If a message box for *Configure SQL Server Agent* pops up, click **OK**.

The SQL 2000 installation is now complete.

Once SQL server 2000 is installed, install the appropriate service pack(s). Refer to How to install SQL Server service packs for additional information.

When the appropriate SQL Server 2000 service pack is installed, create the ICM database and adjust the database setting. Refer to How to create ICM databases for additional information.

Installing SQL Server service packs

SQL Server service packs can be obtained by accessing the Microsoft web site.

How to install SQL Server service packs

Step 1 Download the appropriate SQL Server service pack. (SQL Server 2000 SP2 in this case.)

Step 2 Following the instructions provided with the service pack, install it.

Creating ICM Databases

How to create ICM databases

Step 1 When SQL Server setup and service pack installation is complete, reboot the server.

Step 2 Install the applicable ICM component(s) (Logger, RTD, AW, HDS, etc.) and hot fixes.

a. Refer to the applicable node forms, checklists, and technical documentation for installing ICM software.

Step 3 Verify that SQL Server is running.

Step 4 Select **Start > Run > icmdba**. Use *ICMDBA* to create the appropriate database(s). Directions on how to use this tool can be found in the 5.0 *Cisco ICM Software Administrator Guide*.

You may be prompted that the following items need to be changed:

- Set the *TempDB Size* to at least **50 MB**, then click **OK**.
- Set the *TempDB Log* to at least **20 MB**, then click **OK**.

a. If the local server is not listed, create it by selecting **File > Add Server**

b. Enter the **local server name**.

c. Drill down to the server you are working on.

d. Select the server.

e. Add the data devices by highlighting the disk drive in the device field.

f. Enter the size of the database device.

g. Add the appropriate Log Devices. The size of this device typically should not be larger than 500 MB for most ICM installations.

h. Enable partitioning if applicable.

i. Click **Database > Create**.

Note The amount of time necessary to create the database is dependant on the database size.

Once the database is created, configure SQL Server 2000 by following steps 1-4 (inclusive) of How to configure SQL Server.

Upgrading MS SQL Server 7.0 to MS SQL Server 2000

The SQL Server 7.0 to SQL Server 2000 upgrade is straightforward. Before running SQL Server 2000 setup, however, some Microsoft fixes have to accomplished, otherwise, the upgrade may fail. Two bugs in the Microsoft knowledge database may cause an error during upgrading from SQL 7.0 to SQL 2000.

- Q300676 fixes a race condition when running Message.sql.
- Q285100 fixes connectivity problems over the SQL Server Shared Network Library component.

These bug fixes can be downloaded from Microsoft web site. To apply the bug fix, the files on the SQL Server 2000 installation CD have to be copied to a disk. This is because the bug fix requires replacing a few files on the CD. It is not convenient, but Microsoft has confirmed that it is the only way to apply in the bug fix.

Refer to How to upgrade SQL Server 7.0 to SQL Server 2000, page 7-7 for the upgrade procedure.

How to upgrade SQL Server 7.0 to SQL Server 2000

Step 1 Copy the *SQL Server 2000 Installation CD* to a disk, then add the required fixed from Microsoft.

Step 2 Back up all databases to be upgraded, then verify that the backup is good.

Note Backing up the *cust_awdb* is not required.

Step 3 Using the ICM service control, stop all ICM services on the local server.

Step 4 Make sure no one is using SQL Server 7.0 as the upgrade process turns off the server.

Step 5 Start SQL Server 2000 *autorun.exe*.

Step 6 On the first screen:

a. Select **Install SQL 2000 Server Components**.

b. Select **Install Database Server**.

Step 7 Read the *Welcome* screen, then click **Next**.

Step 8 On the *Computer Name* screen:

a. Make sure the default of **Local Computer** is selected.

b. Click **Next**.

Step 9 On the *Installation Selection* screen:

a. Choose **Upgrade, remove, or add components to an existing instance of SQL Server**.

b. Click **Next**.

Step 10 On the *Instance Name* screen:

a. Make sure **Default** is checked.

b. Click **Next**.

Step 11 On the *Existing Installation* screen:

a. Select **Upgrade your existing installation**.

b. Click **Next**.

Step 12 On the *Upgrade* screen:

a. Check **Yes, upgrade my SQL Server Tools and data**.

b. Click **Next**.

Step 13 On the *Connect To Server* screen:

a. Select **Windows Authentication**.

b. Click **Next**.

Step 14 Read the *Start Copying Files* screen, then click **Next**.

Step 15 On the *Licensing* screen, in the *Choose License Mode* section:

a. Set the licensing method to **per seat.**

b. Set at least **40** devices.

Note If you need to choose Processor License for licensing reasons, make sure there are sufficient concurrent connection licenses to ensure the system does not run into licensing problems. While the precise number depends on the accessing need, there should be at least 40 concurrent connections.

Step 16 If the *Setup is installing Microsoft Data Access Components* screen is shown, click **Next** or **Finish.**

The installation is now complete.

The SQL Server 2000 installation is now complete.

Once SQL server 2000 is installed, install the appropriate service pack(s). Refer to How to install SQL Server service packs for additional information.

How to configure SQL Server

Step 1 Select **Start > Programs > Microsoft SQL Server > Enterprise Manager**.

Step 2 Right click on each DB and select **Properties.** Check the properties of each database in Enterprise manager (the ICM database, the temp database, and the master database).

a. Click on Data Files tag.

b. Set the database size large enough to be sufficient for the foreseeable future if disk space is available.

c. Enable **Automatically grow file**.

d. Set *Automatically grow by percent* to **10%**.

e. Set the *Maximum file size* to **Restrict file growth**. Database file growth is obviously limited by the physical disk space available. It is up to you to set the a suitable maximum size.

Note Setting maximum file size is important because database file growth may potentially use all the disk space and can cause system-wide problems. If the database files are on the system disk (for example C:), it is recommended that the size of all database files should not be over 80% of all the disk space because running out of disk space on the system disk is not a desirable scenario. It is also important to remember that there can be many databases on a single database server and many disk files on a single disk. Each data file should only use its share of disk to avoid running out of disk space. This setting is based on your configuration and is up to you to do the calculation for the limits.

f. Verify correct sizing of each database.

Databases include: ICM logger DB, AW DB, or HDS DB (depending on ICM node)

tempdb should be at least **50 MB**

master db should be at least **50 MB**

g. Verify correct sizing of the *transaction log* for each database.

Databases include: ICM logger DB, AW DB, or HDS DB (depending on ICM node)

Under the *transaction log tab* for each database, **disable auto-grow**.

Note It is recommended that transaction log in ICM system to be kept under 500M to allow rapid recovery in case of restarting the system. Even though the database files are allowed to automatically grow, the size of the transaction log growth should be changed manually.

ICM logger DB, AW DB, or HDS DB transaction log (depending on ICM node).

tempdblog should be at least **20 MB**

master db log should be at least **20 MB**

h. Do not change anything under the *Permissions tab.*

i. Select the *Options tab* and set the options as follows:

ANSI NULL default: **No**

Recursive triggers: **No**

Auto update statistics: **Yes**

Torn page detection: **Yes**

Auto close: **No**

Auto shrink: **No**

Auto create statistics: **Yes**

Use quoted identifier: **No**

All other parameters should be left as default

Step 3 If changes are needed, the MSSQLSERVER Service may need to be cycled.

Step 4 Close SQL Enterprise Manager.

Step 5 Run ICM *setup*.

a. In a command window type: **c:\icr\bin** and press **Enter**.

b. Type **setup**.

c. Select the ICM component (logger or Admin Workstation) being upgraded.

d. Click **Edit**.

e. Click **OK** to proceed through the setup utility.

f. Click **Next** in each window and complete setup without making any changes.

g. Click **Finish** and exit the ICM setup program.

Step 6 Start the upgraded machine.

Step 7 Verify there are no errors in ICM processes or SQL error log.

Cisco Systems

Part 3

ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Upgrade Migration

ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Upgrade Introduction

This section describes the proper procedures for upgrading Cisco Intelligent Contact Management (ICM) 4.6.2 or ICM 5.0(0) systems to ICM/IP Contact Center Enterprise Edition, Release 6.0(0).

The upgrade process may be accomplished using one of two possible methods:

- the ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Common Ground Upgrade Migration method

  The Common Ground Upgrade Migration method involves upgrading on your existing Bill Of Materials (BOM) complient hardware.

- the ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Technology Refresh Upgrade Migration method

  The Technology Refresh Upgrade Migration method involves moving specified data from your existing ICM production system to new Bill Of Materials (BOM) complient hardware.

  This method is based on the following:

  – the new hardware is Cisco ICM Bill of Materials (BOM) compliant

Note See *http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm* for additional ICM/IP Contact Center Enterprise Edition, Release 6.0(0) BOM information.

- the new hardware has MS Windows 2000 SP4 and MS SQL 2000 SP3 installed; and is an Active Directory environment.

Note This document provides the appropriate service pack levels to be used throughout both the Common Ground and the Technoloogy Refresh upgrade methods. Refer to the BOM (*http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm*) for the latest information on current service pack requirements.

Components interfacing with Cisco Intelligent Call Management software not covered in this document:

- CallManager
  - See *Using Cisco CallManager Upgrade Assistant Utility 4.0(1)* and *Upgrading Cisco CallManager Release 4.0(1).*
- IP IVR (Customer Response Applications)
  - See *Getting Started with Cisco Customer Response Applications, Release 3.5*.
- Internet Service Node (ISN)
  - See *Cisco Internet Service Node (ISN), Release 2.1 Installation Guide*.
  - See *Cisco Internet Service Node (ISN), Release 2.1 Release Notes*.
- Computer Telephony Integration Object Server (CTI OS)
  - See the *Cisco ICM Software CTI OS System Manager's Guide*.
- Cisco Agent Desktop (CAD)
  - See Cisco Agent Desktop *Installation Guide (Release 4.6).*

It is necessary, however, to include or consider these components in the overall planning of your Cisco ICM Software upgrade, as certain versions of ICM are compatible with certain versions of the previously mentioned components.

ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Upgrade Planning

Upgrade planning

When planning to upgrade your ICM system, first prepare a:

- Network Inventory
- Data Backup Plan
- Network Configuration Backup
- Default Routing Plan
- Test Plan
- Detailed Schedule of Upgrade Activities
- Definition of Upgrade Steps
- Post-upgrade Test Definition
- Stakeholder Notification

ICM Baseline

Prior to upgrading, the following baseline is necessary when upgrading from an ICM 4.6.2 or an ICM 5.0(0) system to an ICM/IP Contact Center Enterprise Edition, Release 6.0(0) system:

- Cisco ICM 4.6.2 or ICM 5.0(0)

Note If you are upgrading an IPCC system, for additional upgrade information refer to the *Release Planning and Installation/Upgrade Details* section of the *Cisco ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Release Notes*, the *Cisco ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Administration Guide,* and/or the *IPCC Software Compatibility Guide* (see http://www.cisco.com/application/pdf/en/us/partner/products/ps1844/c1609/ccmigration_09186a00801c71)

- Microsoft SQL 7.0 SP3 (for ICM 4.6.2 only) or SP4 (for ICM 5.0(0)only)

  or

  Microsoft SQL 2000 SP3a (for ICM 5.0(0) only)

- Microsoft Windows 2000 SP3

Note Refer to the *Cisco ICM/IP Contact Center Enterprise Edition Windows 2000 Planning for Release 6.0* and the *Cisco ICM/IP Contact Center Enterprise Edition, Release 6.0 Staging on Windows 2000* guides for Windows 2000 planningand staging information.

Hardware recommendations

The ICM system hardware (i.e., hard drive(s), memory, etc.) must meet certain requirements to run ICM software release 6.0(0).

Hardware specifications play a critical part in the successful operation of an ICM system. Audit all hardware prior to the upgrade to determine if a hardware upgrade is required.

First, review the ICM/IP Contact Center Enterprise Edition, Release 6.0(0) hardware and software specifications. The minimum hardware requirements to upgrade to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) is found in the Cisco ICM Bill of Material (BOM).

Note See *http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm* for the ICM/IP Contact Center Enterprise Edition, Release 6.0(0) BOM.

Software requirements

Cisco ICM/IP Contact Center Enterprise Edition, Release 6.0(0) requires the following 3rd party software for each ICM component:

CallRouter

- MS Windows Server SP4
- PCAnywhere 10.5

Logger

- MS Windows Server SP4
- MS SQL 7.0 SP4 or MS SQL 2000 SP3/3a
- PCAnywhere 10.5

Admin Workstation – Real Time Distributor/WebView Server

- MS Windows Server SP4
- MS SQL 7.0 SP4 or MS SQL 2000 SP3/3a
- PCAnywhere 10.5
- Infomaker 8.0.1 (required for ICM WebView custom reporting)
- ICM WebView 3rd Party Software 5.0

Admin Workstation – Real Time Client

- MS Windows Server SP4
- PCAnywhere 10.5
- Infomaker 8.0.1 (required for ICM WebView custom reporting)

Peripheral Gateway

- MS Windows Server SP4
- PCAnywhere 10.5

Related publications

When planning ICM system upgrades, familiarize yourself with Cisco Intelligent Call Management documentation relative to ICM, IPCC, and the Remote Monitoring Suite.

Review and have available the following documents when performing an ICM 4.6.2 or ICM 5.0(0) to an ICM/IP Contact Center Enterprise Edition, Release 6.0(0) system upgrade:

- Cisco ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Documentation Set
- *Cisco ICM/IP Contact Center Enterprise Edition Release Notes, Release 6.0(0)*
- Release notes for the Cisco ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Service Release

CHAPTER 10

ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Common Ground Upgrade Migration

Common Ground ICM Upgrade Migration Events

Introduction

The upgrade migration of an ICM 4.2.6 or ICM 5.0(0) system to an ICM/IP Contact Center Enterprise Edition, Release 6.0(0) system involves numerous steps. From your initial software load, you may need to upgrade the operating system, the ICM software (and options), the database software, and any required third party software.

This chapter provides the following information:

- Common Ground Upgrade Migration Method Overviews
  - ICM 4.6.2 System to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) System Common Ground Upgrade Migration Overview

    This section provides an overview of the tasks required to upgrade from an ICM 4.6.2 system to an ICM/IP Contact Center Enterprise Edition, Release 6.0(0) system using the Common Ground upgrade migration method.

  - ICM 5.0 System to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) System Common Ground Upgrade Migration Overview

    This section provides an overview of the tasks required to upgrade from an ICM 5.0 system to an ICM/IP Contact Center Enterprise Edition, Release 6.0(0) system using the Common Ground upgrade migration method.

- ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Common Ground Upgrade Migration Tasks
  - This section lists and discusses, in general, the tasks required to perform a Common Ground ICM upgrade migration. Detailed discussions of the upgrade migration tasks and steps are found in Common Ground Upgrade Migration Tasks.

Common Ground Upgrade Migration Method Overviews

ICM 4.6.2 System to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) System Common Ground Upgrade Migration Overview

This section provides an overview of the steps required to upgrade from an ICM 4.6.2 system to an ICM/IP Contact Center Enterprise Edition, Release 6.0(0) system using the Common Ground upgrade migration method.

Note For the purposes of this section, it is assumed that side A is the side to be upgraded first.

Central Controllers, AW/HDS and WebView

Step 1 On the AW/HDS, open Script Editor and run **Validate All**.

Step 2 With side B still running ICM 4.6.2 and processing calls, stop side A and perform the following upgrades:

a. ICM 4.6.2 (select the appropriate component) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0)

b. MS SQL 7.0 SP3 to MS SQL 7.0 SP4

c. MS Windows 2000 SP3 to MS Windows 2000 SP4

Step 3 Stop side B.

Step 4 Ensure default routing is operating properly.

Step 5 Start side A – verify stabilization with calls processing (default routing no longer invoked).

Step 6 Perform the following upgrades on side B:

a. ICM 4.6.2 to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) (for each ICM component)

b. MS SQL 7.0 SP3 to MS SQL 2000 SP4

c. MS Windows 2000 SP3to MS Windows 2000 SP4

Step 7 Synchronize the side A Logger with the side B Logger.

Step 8 Start side B.

Step 9 Stabilize with the Peripheral Gateways at ICM 4.6.2 and calls processing.

Peripheral Gateways

Note This sections assumes you have duplex PGs.

Step 1 Stop the side A PG and perform the following upgrades:

a. ICM 4.6.2 (for the PG component) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0)

b. MS Windows 2000 SP3 to MS Windows 2000 SP4

c. CTI OS server 4.7 to CTI OS server 6.0

d. CILTest 4.7 SP3 to CILTest 6.0

e. CallManager Simulator 5.0 to CallManager Simulator 6.0

Step 2 Start the PG(s) and verify stabilization with calls processing.

CallManager, CAD Server and Client, CTI OS Agent and CTI Agent

Step 1 Stop ***CallManager*** and perform the following upgrades:

Note Calls will be stopped during this time period.

a. CCM 3.3.3 to CCM 4.0
b. Publisher 3.3.3 to Publisher 4.0
c. IP IVR 3.1 to IP IVR 3.5
d. MS SQL 2000 SP3 to MS SQL 2000 SP3a
e. MS Windows 2000 SP3 to MS Windows 2000 SP4

Step 2 Stop the ***CAD server and Client***, then perform the following upgrades:

a. CAD server 4.4.1 to CAD server6.0
b. MS SQL 7.0 SP3 to MS SQL 2000 SP3a
c. CAD Client 4.4.1 to CAD Client 6.0
d. MS Windows 2000 SP3 to MS Windows 2000 SP4

Step 3 Stop ***CTI OS Agent and CTI Desktop***, then perform the following upgrades:

a. CTI OS Agent 4.6.2 to CTI OS Agent 6.0
b. CTI Desktop 4.6.2 to CTI Desktop 6.0
c. MS Windows 2000 SP3 to MS Windows 2000 SP4

Step 4 Start ***CallManager***, ***CAD Server and Client***, and ***CTI OS Agent and CTI Desktop***.

Step 5 Start calls and perform post testing.

ICM 5.0 System to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) System Common Ground Upgrade Migration Overview

This section provides an overview of the steps required to upgrade from an ICM 5.0 system to an ICM/IP Contact Center Enterprise Edition, Release 6.0(0) system using the Common Ground upgrade migration method.

Note For the purposes of this guide, it is assumed that side A is the side to be upgraded first.

Central Controllers, AW/HDS and WebView

Step 1 With side B still running ICM 5.0 and processing calls, stop side A and perform the following upgrades:

- **a.** ICM 5.0 (select the appropriate component) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0)
- **b.** MS SQL 7.0 SP4 to MS SQL 2000 SP3a
- **c.** MS Windows 2000 SP3 to MS Windows 2000 SP4

Step 2 Stop side B.

Step 3 Ensure default routing is operating properly.

Step 4 Start side A – verify stabilization with calls processing (default routing no longer invoked).

Step 5 Perform the following upgrades on side B:

- **a.** ICM 5.0 to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) (for each ICM component)
- **b.** MS SQL 7.0 SP4 to MS SQL 2000 SP3a
- **c.** MS Windows 2000 SP3 to MS Windows 2000 SP4

Step 6 Synchronize the side A Logger with the side B Logger.

Step 7 Start side B.

Step 8 Stabilize with the Peripheral Gateways at ICM 5.0 and calls processing.

Peripheral Gateways

Note This sections assumes you have duplex PGs.

Step 1 Stop the side A PG and perform the following upgrades:

a. ICM 5.0 (for the PG component) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0)

b. MS Windows 2000 SP3 to MS Windows 2000 SP4

c. CTI OS server 4.7 to CTI OS server 6.0

d. CILTest 4.7 SP3 to CILTest 6.0

e. CallManager Simulator 5.0 to CallManager Simulator 6.0

Step 2 Start the PG(s) and verify stabilization with calls processing.

CallManager, CAD Server and Client, CTI OS Agent and CTI Agent

Step 1 Stop ***CallManager*** and perform the following upgrades:

Note Calls will be stopped during this time period.

a. CCM 3.3.3 to CCM 4.0

b. Publisher 3.3.3 to Publisher 4.0

c. IP IVR 3.1 to IP IVR 3.5

d. MS SQL 2000 SP2 to MS SQL 2000 SP3a

e. MS Windows 2000 SP3 to MS Windows 2000 SP4

Step 2 Stop the ***CAD server and Client***, then perform the following upgrades:

a. CAD server 4.4.1 to CAD server6.0

b. MS SQL 7.0 SP4 to MS SQL 2000 SP3a

c. CAD Client 4.4.1 to CAD Client 6.0

d. MS Windows 2000 SP3 to MS Windows 2000 SP4 (on both)

Step 3 Stop ***CTI OS Agent and CTI Desktop***, then perform the following upgrades:

a. CTI OS Agent 4.6.2 to CTI OS Agent 6.0

b. CTI Desktop 4.6.2 to CTI Desktop 6.0

c. MS Windows 2000 SP3 to MS Windows 2000 SP4 (on both)

Step 4 Start ***CallManager***, ***CAD Server and Client***, and ***CTI OS Agent and CTI Desktop***.

Step 5 Start calls and perform post testing.

CIS Components

Step 1 Stop the ***CIS components***.

- Cisco Media Blender (CMB)
- Cisco E-mail Manager (CEM)
- Cisco Collaboration Server (CCB)
- Dynamic Content Adapter (DCA)

Step 2 Upgrade the service packs for the operating system and MS SQL Server as indicated for the following CIS components:

- ***CMB 5.0***
  - MS Windows 2000 SP3 to MS Windows 2000 SP4
- ***CEM 5.0***
  - MS SQL 2000 SP2/Oracle 8.1.7 to MS SQL 2000 SP3a/Oracle 8.1.7
  - MS Windows 2000 SP3 to MS Windows 2000 SP4
- **CCS 5.0**
  - MS SQL 2000 SP2/Oracle 8.1.7 to MS SQL 2000 SP3a/Oracle 8.1.7
  - MS Windows 2000 SP3/Solaris 8 to MS Windows 2000 SP4/Solaris 8+
- ***DCA 5.0***
  - MS Windows 2000 SP3 to MS Windows 2000 SP4

Step 3 Start the CIS components and assure the interface with ICM is continued.

Step 4 Stop the ***Support Tools*** nodes and perform the following upgrade:

Note This process does not interrupt any calls or interfere with any other ICM system functionality.

- Support Tools 1.0 to Support Tools 1.1

Step 5 Start the Support Tool nodes.

ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Common Ground Upgrade Migration Tasks

The following is an overview of the tasks involved when upgrading ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0).

Note For the purposes of this guide, it is assumed that side A is the side to be upgraded first.

Step 1 **Perform pre-upgrade activities.**

Step 2 **Stop the Central Controller side A and the Key AW(s) to be upgraded.**

Note Stopping the side A Central Controller (assumed side to be upgraded) puts side B (from a Central Controller prospective) into a simplex condition.

Note The management of domain controllers is critical during the ICM upgrade process. If the domain controller is installed on a node with an ICM component, ensure you upgrade this domain controller's ICM components either prior to, or upon the completion of, the upgrading of all the other ICM nodes.

- The ICM upgrade commences with stopping all ICM services on the side A Central Controller (the side A Logger and the side A Router) and the *Key* Aw(s).
- The side B Router requires successful connectivity with greater than 50% of the configured Peripheral Gateways (PGs) for proper simplex operation.

Step 3 Upgrade the Key Admin Workstation(s)

- *Key* Admin Workstations must be upgraded with the first side of the Central Controller to be upgraded. This is so testing can be completed prior to upgrading the second side of the Central Controller.
- A *Key* AW, from a demographics view, is simply the AW used for system administration located near the Central Controller being upgraded.
- Admin Workstations must be at the same version as the Central Controllers in order to work properly. Before the Central Controller side with the upgraded software is brought online, any AWs left at the older version of software should be shut down to avoid continuously attempting to connect to the upgraded Central Controller. Continuous re-connection attempts are eventually refused, but in the interim cause unnecessary overhead on the Central Controller and the network.

Note No configuration changes are allowed during the upgrade process. Any configuration changes must wait until the upgrade is complete.

Step 4 Upgrade ICM Central Controller side A.

- Side A CallRouter and Logger are upgraded to the new level of software. However, upon completion of the upgrades and reboot of machines, the Logger and CallRouter Services are not started. The upgrade steps include setting all ICM services to manual before proceeding with the upgrade.

Step 5 Stop the non-upgraded Central Controller side B and remaining AWs.

- Stop Central Controller side B. ICM Central Controllers cannot run in duplex mode unless the software levels on sides A and B are identical. Therefore, side B Central Controller must be stopped before the side A Central Controller is started at the new/upgraded software level.

Note Stopping the side B Central Controller puts side A (from a Central Controller prospective) into a simplex condition when the services are started.

Step 6 Short term default routing

- Once all Central Controller services are stopped on side B, start the side A Central Controller services.

  When the side B Central Controller is stopped and the side A Central Controller services are coming on line, the Service Provider's default network routing plan is invoked.

Step 7 **Start up the upgraded side A of the Central Controller**

- The side A CallRouter requires successful connectivity with 50% of the configured PGs for that instance.
- Before proceeding with the upgrade of the B side central controller, testing should be completed with side A in a simplex condition. Only upon successful completion of testing should a "*Go*" decision be made to continue with upgrading the B side central controller.
- To stop the upgrade at this point, stop the ICM software on the upgraded machines and start ICM on the non-upgraded machines. Once the non-upgraded machines are back on line the upgraded machines can be brought back to their original state using the stored image.

Note If any component is not functioning properly, capture the appropriate log for troubleshooting purposes before the old image is restored.

If no issues are identified, or if a problem is assessed as "non-critical" to the business, the upgrade continues.

Step 8 **Upgrade ICM Central Controller side B**

- Only upon successful completion of side A simplex testing should a "*Go*" decision be made to continue with upgrade of the side B Central Controller.
- Once the Central Controller has been successfully upgraded and synchronized, testing should be completed in duplex mode.

Step 9 **Upgrade the remaining Admin Workstation(s)**

- Once the ICM system has been successfully tested, the remaining Admin Workstations may be upgraded and started.

Step 10 Upgrade the Peripheral Gateways.

- Peripheral Gateways may be as many as two releases lower than the Central Controller release. The Peripheral Gateways do not necessarily have to be upgraded during the same maintenance window as the Central Controllers. However, it is strongly recommended that they be upgraded within the same week as the Central Controllers.

Note ICM 4.6.2 PG's are compatible with ICM 6.0 Central Controllers subject to reporting limitations relative to features introduced in the newer version. Upgrade all components to the latest version to take advantage of the newest features.

Step 11 **Upgrade MS SQL Server.**

- It is recommended all operating system and ICM upgrade steps are completed, the historical data migration is complete, and the system is stable prior to performing a SQL upgrade.
  - Verify completion by looking at the *recovery* log on the Logger and the *replication* log on the HDS.
  - In addition, verify the completion of the configuration transfer to the Router using the Router Router and Logger Logger logs; AW Update using the Update AW and Logger Logger logs; HDS data replication using the HDS Replication and Logger Recovery logs.
- Upgrade MS SQL 7.0 SP3/4 to MS SQL 2000 SP3a. (See How to upgrade SQL Server 7.0 to SQL Server 2000, page 12-8.)

Note **For ICM 4.6.2 to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) upgrades only:** Be aware that when you run ICM *setup.exe*, the automatic conversion of the registry keys (from *GeoTel* to *Cisco Systems, Inc.*, and *icr* to *icm*) occurs before you gain access to the *ICM Setup* dialog.

Common Ground Upgrade Migration Tasks

Note For the purposes of this guide, it is assumed that side A is the side to be upgraded first.

Common Ground Upgrade Migration Task Overview

Caution **Perform the upgrade migration tasks in the order listed.**

Note Refer to the appropriate section of the following Common Ground Upgrade Migration Task - Detailed Steps for the steps for the following tasks.

Note Perform all tests included in the test plan, system and application tests before and after the upgrade.

Note Prior to commencing the upgrade, it is recommended you reboot each machine in the ICM system and verify all services return to the expected status. Fail-over functionality can also be verified this way as well.

Caution **Do not proceed with the upgrade if you encounter any problems completing the pre-upgrade activities.**

After reviewing and approving your migration plan (see Upgrade Planning), complete the following pre-upgrade activities:

1. Validate the system infrastructure.
   a. Verify the status of each ICM instance.

b. Confirm that the Logger databases are no more than 65-70% full (30-35% free space). See Determine the Occupied Space in the Logger/HDS Database.

c. Confirm that the HDS databases are no more than 50% full (50% free space). See Determine the Occupied Space in the Logger/HDS Database.

d. Ensure the C: drive has adequate space for operating system expansion, temporary space, and ICM expansion on all the machines.

   Also ensure you have enough disk space where ever you intend to back up your registry and ICM folder backups, as well as your database backups. Check your database size and base the value for the required disk space on this.

2. Synchronize the Logger Databases
3. Notify the stakeholders of the upgrade schedule.
4. Disable any automatic nightly backups.
5. Make the *Go/No Go* decision to start the upgrade.

- The *Go/No Go* decision is dependent upon the state of the system and the environment.

6. Perform System Backups.
7. Disable Configuration Changes.
8. Backup the GeoTel (ICM 4.6.2) or Cisco Systems, Inc. (ICM 5.0(0)) Registry on all servers.
9. Backup Custom Templates and Reports (optional).

Note If required, arrange with the appropriate resources to backup and restore custom reports. In addition, schedule the appropriate resources to assess custom CTI functionality after an upgrade.

10. Run Pre-upgrade tests

- Application test
  - Validating Scripts
- System Integrity Tests
  - Process testing

- Redundancy testing
- Alarm testing
- Historical reporting testing
- WebView reporting testing (option)
- Internet Script Editor testing (option)

11. Stop ICM side A
12. Upgrade the side A Key Admin Workstation(s)

Note If there is only one AW/HDS in the enterprise, start the upgrade with the corresponding Central Controller side.

13. Upgrade the ICM side A Central Controller
14. Stop ICM side B and remaining AWs
15. Validate network default routing
16. Start ICM side A and the Key AW
17. Validate ICM side A routing is restored
18. Make the Go/No Go decision to upgrade ICM side B
19. Upgrade the side B Key Admin Workstation
20. Upgrade the ICM side B Central Controller
21. Start ICM side B
22. Upgrade the remaining AWs
23. Ensure the Configuration database transfer is complete
24. Enable configuration updates
25. Run Post-Upgrade tests
    a. Application test
       - Validate Scripts
    b. System Integrity Tests
       - Process testing
       - Redundancy testing

- Alarm testing
- Historical reporting testing
- WebView reporting testing (option)
- Internet Script Editor testing (option)

26. Upgrade the Peripheral Gateways (PGs)
27. Upgrade MS SQL Server (optional - refer to ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) SQL Server Installation and Upgrade, page 12-1)
28. Set all ICM Services to Automatic start.
29. Stakeholder Notification

Common Ground Upgrade Migration Task - Detailed Steps

Verify the status of each ICM instance

Step 1 At the command prompt, run **rttest** on each CallRouter by entering:

rttest /<*cust instance name*>/node CallRouter<*x*>/<*system hostname*>

Note For additional information, see the **rttest** utility Tech Note at: http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1001/products_tech_note09186a00800ac69b.shtml.

Step 2 Confirm that the entire ICM network infrastructure is intact and that all PGs can see and be seen by both sides of their respective CallRouter.

Step 3 If any ICM system problems are observed, address them prior to preceding with the upgrade.

Synchronize the Logger Databases

Prior to starting Logger B, synchronize the side B Logger database with the side A Logger database using ICMDBA.

Step 1 Select **Start > Run**.

Step 2 In the *Run* dialog, type **icmdba**, click **OK**.

Step 3 Select the **ICM instance** in the **icmdba** GUI.

Step 4 Drill down to and select the Logger database.

Step 5 On the tool bar select **Data > Synchronize**.

Step 6 Select the **Source**.

a. Select the previously upgraded and running **Server** and **Database**.

Step 7 Select the **Target**.

a. Select the **Server** and **Database** to be started.

Step 8 Click **Synchronize**.

Step 9 In the *Synchronize* dialog click **Start**.

Step 10 When the message appears indicating the successful completion of the synchronization process, acknowledge it.

Step 11 Close **icmdba**.

Determine the Occupied Space in the Logger/HDS Database

Step 1 Select **Start > Run**.

Step 2 In the *Run* dialog, type **icmdba**, click **OK**.

Step 3 Drill down to the Logger/HDS database.

Step 4 Right-click **<*cust*>_side<*X*>** or **<*cust*>_HDS** (as applicable) and select **Properties**.

Step 5 Ensure *Data % Used* is not above 65% for the Logger and 50% for the HDS.

Step 6 Ensure *Log % Used* is sized to a minimum of 400 MB (500 MB max.).

Step 7 Ensure the tempdb is sized to 100 MB.

Step 8 Increase SQL locks to 200,000. The SQL server service must be recycled in order for this change to take place.

Perform System Backups

The ICM nodes should not be upgraded until preparations have been made to revert the nodes back to their original version of the ICM software in the unlikely case of a catastrophic failure during the upgrade migration. It is recommended that each ICM node be imaged using commercial imaging software.

Disable Configuration Changes

Disabling configuration updates is accomplished by setting a registry variable for each side of the CallRouter to disallow any updates (updates are prevented and an error message is returned).

Make the following registry change on the CallRouter:

```
HKEY_LOCAL_MACHINE\Software\
Cisco\ICM\<instance name>\RouterA\Router\
CurrentVersion\Configuration\Global\
DBMaintenance = 1.
```

Test configuration updates are now disabled.

Backup the GeoTel (ICM 4.6.2) or Cisco Systems, Inc. (ICM 5.0(0)) Registry

Saving the registry is done automatically when **Upgrade All** is run. However, to perform this manually, do the following:

Step 1 Open a command prompt and type **regedit** or use **Start > Run> regedit**.

Step 2 Select **HKEY_LOCAL_MACHINE\SOFTWARE\<*GeoTel or Cisco Systems, Inc.*>\icm**

Step 3 On the tool bar, click **Registry > Export registry file**

Step 4 Browse the directory to determine where you want to export the registry file to.

Step 5 Enter a **filename** that will be remembered.

Step 6 Click **Save**.

Backup Custom Templates and Reports

Backing up custom templates and reports is optional, but recommended when performing a Common Ground upgrade migration.

For ICM 4.6.2 only:

- Backup custom templates by copying: *icm\instancename\aw\custom*.
- Backup saved reports by copying: *icm\instancename\dis\web\userdata*.

Note The ICM 5.0(0) has a WebView database that should be backed up whenever an ICM database backup is performed.

Run Pre-upgrade tests

A test plan is utilized at various stages of the upgrade process. It is up to you to develop the actual test cases with actual dialed numbers, labels, targets, and expected results. The key areas in which to develop test cases follow.

Application test

The most crucial test is the ability of the system to route calls to defined peripheral targets. Side A of the ICM system is upgraded to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) first, then returned to service. Monitor the ICM call routing decisions to determine if it is making the appropriate routing decisions. The Key AWs, upgraded prior to the side B Central Controller, are used to monitor call routing.

Validating Scripts

Step 1 Open *Script Editor.*

Step 2 Select **Script > Validate All** (or click **Validate All** in the tool bar).

Step 3 Observe all scripts are functioning properly. Make note of any scripts having issues prior to the upgrade. Save and compare this information with the post-upgrade script validation results.

System Integrity Tests

The remaining tests are performed to ensure proper functionality of all system components when the ICM is running in duplex mode. Give special attention to redundancy testing.

Process testing

Validate processes on the ICM system. For example, check the following processes for:

RTR - *all configuration data transferred from logger*

LGR - *completed initialization*

AW - *updateAW has completed update and waiting work*

Step 1 Ensure each software process is running properly.

Step 2 Check each NIC for the proper connection to the carrier (IXC) network.

Step 3 Halt and restart each process.

Redundancy testing

Step 1 Stop each active PG to ensure that the back-up PG assumes an active state.

Step 2 Stop the active CallRouter side to ensure that the system switches to the alternate CallRouter side without loss of functionality.

Step 3 Perform the same tests on the logger and the NIC.

Alarm testing

Step 1 Verify your Network Operations Center (responsible for Alarm Tracker monitoring of the system) is receiving the alarms in their tracking system.

Historical reporting testing

Step 1 Launch queries against the upgraded Loggers to ensure the presence and integrity of historical call detail.

WebView reporting testing (option)

Step 1 Open the commonly used WebView views.

Step 2 Examine the data presented.

Internet Script Editor testing (option)

Step 1 Open the most commonly monitored ICM scripts using Internet Script Editor.

Step 2 Examine the data presented.

Stop ICM side A

Step 1 **Stop** the side A Central Controller and AW/HDS using the local service control. Set all ICM services to **Manual**.

Step 2 On an AW on the still running side of the old production system, use Script Editor to monitor call routing. Confirm that calls are **not** being default routed. If they are **not**, the upgrade of side A can begin.

Upgrade the side A *Key* Admin Workstation(s)

If there is only one AW/HDS in the enterprise, start the upgrade with the corresponding Central Controller side.

Step 1 Ensure the Distributor services are stopped and set to **Manual** in the *Service* dialog.

Step 2 If this is a WebView Server, run **setup.exe** from the *WebView 3rd Party Software CD*.

Note **When upgrading ICM 4.6.2 to ICM/IP Contact Center Enterprise Edition, Release 6.0(0):**
1. Upgrade the Third Party Tools
2. Run ICM Setup.exe to upgrade the ICM.

Note **When upgrading ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0):**
1. Third Party Tools remain the same, no upgrade required.
2. Run ICM **setup.exe** to upgrade the ICM.

Note If you get a *Read Only File Detected* dialog, click **Do not display this message again**, then click **Yes**.

Step 3 Run ICM **setup.exe** from the ICM Installation CD.

Note **When upgrading ICM 4.6.2 to ICM/IP Call Center Enterprise Edition, Release 6.0(0)**, the following message is displayed in the *Question* window:

Setup is about to convert GeoTel registry to Cisco registry and rename icr directory to icm directory. After the conversion, please perform upgrade to all on the icm system. Do you want to continue?

Select **Yes**.

Step 4 Select **Upgrade All**. The *Upgrade all ICM instances* dialog appears.

Step 5 Press **OK** to upgrade all instance components of this system.

Step 6 If you have WebView, a dialog appears asking for the location of WebView Server. Enter the **DB Server machine name** and click **OK**.

Note If you get a *Read Only File Detected* dialog, click **Do not display this message again**, then click **Yes**.

Step 7 Reboot as directed.

Note The ICM processes should not be started until after the Central Controller Side A has been upgraded.

Upgrade the ICM side A Central Controller

Step 1 From the Cisco ICM media, run ICM **setup** to first upgrade the side A Router, then the side A Logger. Select **Upgrade All** for each.

Step 2 On the *Question* screen the following message is displayed:

Setup is about to convert GeoTel registry to Cisco registry and rename icr directory to icm directory. After the conversion, please perform upgrade to all on the icm system. Do you want to continue?

Select **Yes**.

Step 3 Select **Upgrade All**. The *Upgrade all ICM instances* dialog appears.

Step 4 Press **OK** to upgrade all instance components of this system.

Caution Do not proceed if the upgrade states that it cannot remove files from the \icm\bin directory.

The files left in the \icm\bin directory are the ones that could not be removed. Typically, this is caused by *rttest.exe* running in the background. To fix this, do the following:

a. Start the *Task Manager* by right-clicking on the task bar and choosing **Task Manager**.

b. Select the **Processes** tab then right click on *rttest.exe* and select **End Task**. Look for multiple instances of this process running in task manager.

c. Once finished, reboot each machine as requested by *setup*. Remember, delay rebooting the Logger until the Router is fully upgraded.

Note If the Restart Windows dialog appears with the message:
Some files could not be updated because they are currently in use by other programs on the system. Files in use will be updated the next time you restart the system.
Select **Yes, I want to restart my computer now**, then **OK**.

Step 5 Apply any Service Releases or Engineering Specials as directed by the Release Notes.

Step 6 Ensure that the side A machines have returned no errors following the upgrade and the subsequent reboot.

a. Check the log for errors. The **icmsetup.log** file is located in the C:\temp directory. Change to the C:\temp directory and perform the following command line checks.

- Search for errors using: **findstr /i error icmsetup.log**.

Note No response indicates no errors were found.

- Search for failures using: **findstr /i fail icmsetup.log**.

Note No response indicates no failures were found.

- Search for errors using: **findstr /i warning icmsetup.log**.

Note No response indicates no warnings were found.

- If you wish, review the log in *Notepad* using: **notepad icmsetup.log**.

Stop ICM side B and remaining AWs

To stop ICM side B:

Step 1 **Stop** the side B Router, Logger, and AW/HDS (in that specific order) using the local service control. Set all ICM services to **Manual**.

Note Stop all services individually. Do not use the **Stop All** option.

Validate network default routing

To validate network default routing:

Step 1 Refer the local *Service Control* dialog and ensure both the side A and side B Router and Logger services are stopped and set to manual.

Step 2 Validate that *Network Default Routing* is taking place.

Start ICM side A and the *Key* AW

Step 1 Using local service control, start the side A Logger and Router.

Step 2 Once the side A Logger and Router initilization is complete, start the AW/HDS.

Note Start the services individually. Do not use the *Start All* option.

Note After the upgrade, there may be two *ICM Service Control* icons on the desktop. Right-click on each and select **Properties**. Delete the icon having *icr* in the *Target* and *Start in* fields. Use the *ICM Service Control* icon with *icm* in the *Target* and *Start in* fields.

Step 3 Look for the UAW (*UpdateAW.exe*) process running in the desktop task bar with the line *Nothing to do.* At this point, its configuration should match that of the logger and all the standard tools should be usable.

If this AW is a Real-Time Distributor (RTD), the last line of the RTDist process running in the desktop task bar should state *Preferred DB restored.*

Validate ICM side A routing is restored

Step 1 Enable configuration updates for all instances by setting the following registry variable in the CallRouter.

```
HKEY_LOCAL_MACHINE\Software\
Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\
CurrentVersion\Configuration\Global\
DBMaintenance = 0.
```

Step 2 Run simplex tests to check:

a. Call routing

b. AW configuration and scripting

c. Using Script Editor, run **Validate All**.

d. WebView and Internet Script Editor access by a pre-upgrade and a post-upgrade created user.

When these checks are completed, refer to Make the Go/No Go decision to upgrade ICM side B.

Make the *Go/No Go* decision to upgrade ICM side B

If the tests to validate that ICM side A routing is restored are successful and the decision is to proceed (*Go*), then continue to the next section - Upgrade the side B Key Admin Workstation.

If tests to validate that ICM side A routing is restored are not successful and the decision is not to go forward (*No Go*) then:

Step 1 Stop ICM side A.

Step 2 Start up ICM side B.

Step 3 Revert ICM side A back to the prior release using the saved image.

Step 4 Restart side A.

Step 5 Enable configuration updates for all instances by setting the registry variable in the CallRouter. The following registry change should be made on the CallRouter:

```
HKEY_LOCAL_MACHINE\Software\
GeoTel\ICR\<instance name>\RouterA\Router\
CurrentVersion\Configuration\Global\
DBMaintenance = 0.
```

Upgrade the side B *Key* Admin Workstation

Step 1 Disable configuration changes by making the following registry change on the CallRouter:

```
HKEY_LOCAL_MACHINE\Software\
GeoTel\ICR\<instance name>\RouterA\Router\
CurrentVersion\Configuration\Global\
DBMaintenance = 1.
```

Step 2 Ensure the Distributor services are stopped, then set them to **Manual**.

Step 3 If this is a WebView Server, run **setup.exe** from the *WebView 3rd Party Software CD*.

Note **For ICM 4.6.2 to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) upgrades only:** Be aware that when you run ICM *setup.exe*, the automatic conversion of the registry keys (from *Geotel* to *Cisco Systems, Inc.*, and *icr* to *icm*) occurs before you gain access to the *ICM Setup* dialog.

Note If you get a *Read Only File Detected* dialog, click D**o not display this message again**, then click **Yes**.

Step 4 Run ICM **setup.exe** from the ICM Installation CD.

Step 5 In the *Question* window the following message is displayed:

Setup is about to convert GeoTel registry to Cisco registry and rename icr directory to icm directory. After the conversion, please perform upgrade to all on the icm system. Do you want to continue?

Select **Yes**.

Step 6 Select **Upgrade All**. The *Upgrade all ICM instances* dialog appears.

Step 7 Press **OK** to upgrade all instance components of this system.

Step 8 If you have WebView, a dialog appears asking for the location of WebView Server. Enter the **DB Server machine name** and click **OK**.

Note If you get a *Read Only File Detected* dialog, click D**o not display this message again**, then click **Yes**.

Step 9 Reboot as directed.

Note The ICM processes should not be started until after the Central Controller Side B has been upgraded.

Upgrade the ICM side B Central Controller

Step 1 From the Cisco ICM media, run ICM **setup** to first upgrade the side B Router, then the side B Logger. Select **Upgrade All** for each.

Step 2 On the *Question* screen the following message is displayed:

Setup is about to convert GeoTel registry to Cisco registry and rename icr directory to icm directory. After the conversion, please perform upgrade to all on the icm system. Do you want to continue?

Select **Yes**.

Step 3 Select **Upgrade All**. The *Upgrade all ICM instances* dialog appears.

Step 4 Press **OK** to upgrade all instance components of this system.

Caution Do not proceed if the upgrade states that it cannot remove files from the \icm\bin directory.

The files left in the \icm\bin directory are the ones that could not be removed. Typically, this is caused by *rttest.exe* running in the background. To fix this, do the following:

a. Start the *Task Manager* by right-clicking on the task bar and choosing **Task Manager**.

b. Select the **Processes** tab then right click on *rttest.exe* and select **End Task**. Look for multiple instances of this process running in task manager.

c. Once finished, reboot each machine as requested by *setup*. Remember, delay rebooting the Logger until the Router is fully upgraded.

Note If the Restart Windows dialog appears with the message:
Some files could not be updated because they are currently in use by other programs on the system. Files in use will be updated the next time you restart the system.
Select **Yes, I want to restart my computer now**, then **OK**.

Step 5 Apply the necessary Service Releases or Engineering Specials as directed by the Release Notes.

Step 6 If Web View is installed, ensure the *web* process has started.

Step 7 Ensure that the side A machines have returned no errors following the upgrade and the subsequent reboot.

a. Check the log for errors. The **icmsetup.log** file is located in the C:\temp directory. Change to the C:\temp directory and perform the following command line checks.

- Search for errors using: **findstr /i error icmsetup.log**.

Note No response indicates no errors were found.

- Search for failures using: **findstr /i fail icmsetup.log**.

Note No response indicates no failures were found.

– Search for errors using: **findstr /i warning icmsetup.log**.

Note No response indicates no warnings were found.

– If you wish, review the log in *Notepad* using: **notepad icmsetup.log**.

Note If Support Tools are installed, you may view any logs using Support Tools from any service starting with ICM release 5.0(0) and higher.

Start ICM side B

Step 1 Using local service control, start the ICM side B services in the following order:

a. Router

b. Logger

c. AW/HDS

Note Start the services individually. Do not use the *Start All* option.

Upgrade the remaining AWs

Step 1 Ensure the Distributor/Client services are stopped, then set them to **Manual**.

Step 2 If this is a WebView Client, run **setup.exe** from the *WebView 3rd Party Software CD* to install *Enterprise Agent Server 4.1.1, JDK 1.3.1, Jaguar CTS 4.1.1,* and *New Atlanta ServletExec ISAPI 4.1.1*.

Note If you attempt to upgrade the AW prior to performing this step, you get a message indicating which of the applications is missing and requires installation.

Note If you get a *Read Only File Detected* dialog, click D**o not display this message again**, then click **Yes**.

Step 3 Run ICM **setup.exe** from the ICM Installation CD.

Step 4 In the *Question* window the following message is displayed:

Setup is about to convert GeoTel registry to Cisco registry and rename icr directory to icm directory. After the conversion, please perform upgrade to all on the icm system. Do you want to continue?

Select **Yes**.

Step 5 Select **Upgrade All**. The *Upgrade all ICM instances* dialog appears.

Step 6 Press **OK** to upgrade all instance components of this system.

Step 7 If you have WebView, a dialog appears asking for the location of WebView Server. Enter the **hostname** and click **OK**.

Note If you get a *Read Only File Detected* dialog, click D**o not display this message again**, then click **Yes**.

Step 8 Reboot as directed.

Note The ICM processes should not be started until after the Central Controller Side B has been upgraded.

Note **Ensure the database migration is complete prior to continuing the upgrade.**

Ensure the Configuration database transfer is complete

Ensure the migration of the Configuration database transfer to the Router and AW update are complete prior to proceeding with the upgrade. HDS can be running in the background while the ICM is used.

Enable configuration updates

Step 1 Enable configuration updates for all instances by setting the registry variable in the CallRouter. The following registry change should be made on the CallRouter:

```
HKEY_LOCAL_MACHINE\Software\
Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\
CurrentVersion\Configuration\Global\
DBMaintenance = 0.
```

Step 2 Test that configuration updates have been enabled.

Run Post-Upgrade tests

A test plan is utilized at various stages of the upgrade process. It is up to you to develop the actual test cases with actual dialed numbers, labels, targets, and expected results. The key areas in which to develop test cases follow. Refer to Run Pre-upgrade tests for additional information on the following tests:

- Application test
  - Validate Scripts
- System Integrity Tests
  - Process testing
  - Redundancy testing
  - Alarm testing
  - Historical reporting testing
  - WebView reporting testing (option)
  - Internet Script Editor testing (option)

Note It may be necessary to run additional tests as required due to the new ICM/IP Contact Center Enterprise Edition, Release 6.0 functionality.

Validate Scripts

Step 1 Open *Script Editor.*

Step 2 Select **Script > Validate All** (or click **Validate All** in the tool bar).

Step 3 Observe all scripts are functioning properly. Make note of any scripts not operating properly after the upgrade, then compare these to the list generated prior to the upgrade.

Upgrade the Peripheral Gateways (PGs)

Note If upgrade planning determines there are redundant PGs, ensure the redundant PGs are up and running properly prior to upgrading the primary PGs.

To upgrade the PGs:

Step 1 When the ICM system (the Router, Logger, and AW/HDS) have stabilized, shut down each primary PG as you intend to upgrade it.

Step 2 Run ICM **setup.exe** (from the media) on each primary PG.

Step 3 In the *Question* window the following message is displayed:

Setup is about to convert GeoTel registry to Cisco registry and rename icr directory to icm directory. After the conversion, please perform upgrade to all on the icm system. Do you want to continue?

Step 4 Select **Upgrade All**. The *Upgrade all ICM instances* dialog appears.

Step 5 Press **OK** to upgrade all instance components of this system.

Caution Do not proceed if the upgrade states that it cannot remove files from the \icm\bin directory.

The files left in the \icm\bin directory are the ones that could not be removed. Typically, this is caused by *rttest.exe* running in the background. To fix this, do the following:

a. Start the *Task Manager* by right-clicking on the task bar and choosing **Task Manager**.

b. Select the **Processes** tab then right click on *rttest.exe* and select **End Task**. Look for multiple instances of this process running in task manager.

c. Once finished, reboot each machine as requested by *setup*. Remember, delay rebooting the Logger until the Router is fully upgraded.

Note If the Restart Windows dialog appears with the message:
Some files could not be updated because they are currently in use by other programs on the system. Files in use will be updated the next time you restart the system.
Select **Yes, I want to restart my computer now**, then **OK**.

Step 6 Apply any Service Releases or Engineering Specials as directed by the Release Notes.

Step 7 Start the PG processes using ICM Service Control.

Step 8 Ensure that the PGs have returned no errors following the upgrade and the subsequent reboot.

a. Check the log for errors. The **icmsetup.log** file is located in the C:\temp directory. Change to the C:\temp directory and perform the following command line checks.

- Search for errors using: **findstr /i error icmsetup.log**.

Note No response indicates no errors were found.

- Search for failures using: **findstr /i fail icmsetup.log**.

Note No response indicates no failures were found.

- Search for errors using: **findstr /i warning icmsetup.log**.

Note No response indicates no warnings were found.

- If you wish, review the log in *Notepad* using: **notepad icmsetup.log**.

b. For other general errors the person performing the upgrade would need to:
   - Identify the condition (for example, ICM service window left open, file in use, etc.)
   - Correct the problem.
   - Run setup again.

c. For SQL errors the person performing the upgrade would need to:
   - Identify the error/errors present in the ICM setup log.
   - Correct the condition.
   - Restore the original database.
   - Run setup again.

Upgrade MS SQL (optional)

Refer to Upgrading MS SQL Server 7.0 to MS SQL Server 2000, page 12-8 for details MS SQL upgrade information and detailed steps.

Set all ICM Services to Automatic start.

Step 1 Double-click the local **ICM Service Control** icon on each ICM component.

Step 2 Select each ICM Service and set it to **Automatic start**.

Notify stakeholders

Notify the stakeholders that the upgrade migration is complete (see Stakeholder Notification).

Upgrading Localized ICM 5.0 Installations to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Installations

If you were running a Japanese, Simplified Chinese or Korean localized version of ICM Release 5.0, to complete the upgrade to a localized version of ICM/IP Contact Center Enterprise Edition, Release 6.0(0):

Step 1 Start **setup.exe** from the ICM/IP Contact Center Enterprise Edition, Release 6.0(0) media.

Step 2 On the *Setup* dialog, in the *Instance component, s*elect **AW**.

Step 3 Click **Edit**.

Step 4 On the *Admin Workstation Properties* dialog select the appropriate language.

Step 5 Click **Next** on all the following dialogs to complete the AW component instance edit.

Step 6 On the *Setup* dialog, click **Upgrade All**.

CHAPTER 11

ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Technology Refresh Upgrade Migration

Technology Refresh Upgrade Migration Events

Introduction

The upgrade migration of an ICM 4.6.2 or ICM 5.0(0) system to an ICM/IP Contact Center Enterprise Edition, Release 6.0(0) system involves numerous steps. From your initial software load, you must upgrade the operating system, the ICM software (and options), the database software, and any required third party software.

This chapter provides the following information:

- Technology Refresh Upgrade Migration Method Overviews
  - ICM 4.6.2 System to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) System Technology Refresh Upgrade Migration Overview

    This section provides an overview of the tasks required to upgrade from an ICM 4.6.2 system to an ICM/IP Contact Center Enterprise Edition, Release 6.0(0) system using the Technology Refresh upgrade migration method.

  - ICM 5.0 System to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) System Technology Refresh Upgrade Migration Overview

    This section provides an overview of the tasks required to upgrade from an ICM 5.0 system to an ICM/IP Contact Center Enterprise Edition, Release 6.0(0) system using the Technology Refresh upgrade migration method.

- ICM Technology Refresh Upgrade Tasks
  - This section lists and discusses, in general, the tasks required to perform a Technology Refresh ICM upgrade migration. Detailed discussions of the upgrade migration tasks and steps are found in ICM Technology Refresh Upgrade Tasks.

Technology Refresh Upgrade Migration Method Overviews

ICM 4.6.2 System to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) System Technology Refresh Upgrade Migration Overview

This section provides an overview of the steps required to upgrade from an ICM 4.6.2 system to an ICM/IP Contact Center Enterprise Edition, Release 6.0(0) system using the Technology Refresh upgrade migration method.

Central Controllers, AW/HDS and WebView

Step 1 Leave the existing ICM system in production and taking calls.

Step 2 On all the new BOM complient Central Controller, AW/HDS, and WebView machines, install:

a. MS Windows 2000 SP4

b. MS SQL 2000 SP3a

a. ICM/IP Contact Center Enterprise Edition, Release 6.0(0) (for the appropriate ICM component)

Peripheral Gateways

Step 1 On the new BOM complient IPCC PG machine(s), install:

a. MS Windows 2000 SP4

b. ICM/IP Contact Center Enterprise Edition, Release 6.0(0) (for the PG component)

c. CTI OS server 6.0

d. CILTest 6.0

CallManager, CAD Server and Client, CTI OS Agent and CTI Agent

Step 1 On all the new BOM complient CallManager, CAD Server and Client, CTI OS Agent and CTI Agent machines, install:

a. MS Windows 2000 SP4

Step 2 On the ***CallManager*** machine(s), also install:

a. MS SQL 2000 SP3a

b. CCM 4.0

c. Publisher 4.0

d. IP IVR 3.5

Step 3 On the ***CAD Server and Client*** machine(s), also install:

a. MS SQL 2000 SP3a

b. CAD Server 6.0

c. CAD Client 6.0

Step 4 On the ***CTI OS Agent and CTI Desktop*** machine(s), also install:

a. CTI OS Agent 6.0

b. CTI Desktop 6.0

ICM 5.0 System to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) System Technology Refresh Upgrade Migration Overview

This section provides an overview of the steps required to upgrade from an ICM 5.0 system to an ICM/IP Contact Center Enterprise Edition, Release 6.0(0) system using the Technology Refresh upgrade migration method.

Central Controllers, AW/HDS and WebView

Step 1 Leave the existing ICM system in production and taking calls.

Step 2 On all the new BOM complient Central Controller, AW/HDS, and WebView machines, install:

- **a.** MS Windows 2000 SP4
- **b.** MS SQL 2000 SP3a
- **a.** ICM/IP Contact Center Enterprise Edition, Release 6.0(0) (for the appropriate ICM component)

Peripheral Gateways

Step 1 On the new BOM complient IPCC PG machine(s), install:

- **a.** MS Windows 2000 SP4
- **b.** ICM/IP Contact Center Enterprise Edition, Release 6.0(0) (for the PG component)
- **c.** CTI OS server 6.0
- **d.** CILTest 6.0

CallManager, CAD Server and Client, CTI OS Agent and CTI Agent

Step 1 On all the new BOM complient CallManager, CAD Server and Client, CTI OS Agent and CTI Agent machines, install:

- **a.** MS Windows 2000 SP4

Step 2 On the ***CallManager*** machine(s), also install:

a. MS SQL 2000 SP3a

b. CCM 4.0

c. Publisher 4.0

d. IP IVR 3.5

Step 3 On the ***CAD Server and Client*** machine(s), also install:

a. MS SQL 2000 SP3a

b. CAD Server 6.0

c. CAD Client 6.0

Step 4 On the ***CTI OS Agent and CTI Desktop*** machine(s), also install:

a. CTI OS Agent 6.0

b. CTI Desktop 6.0

CIS Components

Step 1 On all the BOM complient ***CIS components***, install the following:

- ***Cisco Media Blender (CMB)***
  - MS Windows 2000 SP4
  - CMB 5.0
- ***Cisco E-mail Manager (CEM)***
  - MS Windows 2000 SP4
  - MS SQL 2000 SP3a or Oracle 8.1.7
  - CEM 5.0

- ***Cisco Collaboration Server (CCS)***
  - MS Windows 2000 SP4 or Solaris 8+
  - MS SQL 2000 SP3a or Oracle 8.1.7
  - CCS 5.0
- ***Dynamic Content Adapter (DCA)***
  - MS Windows 2000 SP4
  - DCA 5.0

Step 2 On the ***Support Tools*** nodes, install:

- Support Tools 1.1

ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) Technology Refresh Upgrade Migration Tasks

The Technology Refresh method of ICM upgrade migration involves building a new system at the required Cisco ICM/IP Contact Center Enterprise Edition, Release 6.0(0) hardware and software levels.

To accomplish this upgrade you must:

- Load the new hardware with:
  - MS Windows 2000 SP4
  - MS SQL 2000 SP3a
  - the ICM 4.6.2 or ICM 5.0(0) registry (as applicable)
  - the Logger database
  - the HDS database
  - the AW database
  - Custom templates and saved reports (ICM 4.6.2 only)
  - Third Party Tools (for WebView only)
  - WebView database (if custom templates exist - ICM 5.0(0) only)

  - custom databases
- Install ICM/IP Contact Center Enterprise Edition, Release 6.0(0).
- Move users to the new domain

The Technology Refresh method is accomplished by loading software on the new machines in the following order:

1. Logger (see Logger Technology Refresh upgrade)
2. CallRouter (see CallRouter Technology Refresh upgrade)
3. Admin Workstation (see AW Technology Refresh upgrade)
4. HDS (see HDS Technology Refresh upgrade)

All other components (including PGs) (see All other component Technology Refresh upgrades (PG included))

ICM Technology Refresh Upgrade Tasks

Logger Technology Refresh upgrade

How to Technology Refresh upgrade the Logger

Step 1 Install Windows 2000 SP4.

Step 2 Install Active Directory (on same or separate machine).

Step 3 Set up and configure DNS.

Step 4 Configure a Domain Controller (on same or separate machine).

Step 5 Join the domain.

Step 6 Install MS SQL Server 7.0 SP4 or MS SQL Server 2000 SP3a.

Step 7 Create a MS SQL Server backup of the production logger database.

Step 8 Create the Logger database.

a. Open **MS SQL Enterprise Manager** on the new system.

b. Expand **Microsoft SQL Servers** and **SQL Server Group**.

c. Expand your current ***server name***.

d. Highlight **Databases**.

e. Right-click and select **New Database**.

f. Enter the new ***database name*** and set the initial ***database size*** in MB.

Note The size depends upon the size of the existing database on the old hardware.

g. Click the **Transaction Log** tab and enter the initial log size in MB.

Note The size depends upon the size of the existing log on the old hardware.

h. Click **OK**.

Step 9 Restore the MS SQL Server backup onto the new logger using MS SQL backup /restore.

Note Depending upon the version you initially installed, the data file directories are located in a top level directory named either MSSQL or MSSQL7. When restoring the data files, the MS SQL Server Restore function defaults to MSSQL for this directory name. If necessary, manually input the correct path (example, MSSQL7) during the Restore function so that it matches the actual directory name.

Step 10 Export the ICM 4.6.2 or the ICM 5.0(0) registry key tree from the production logger.

Step 11 Import the ICM 4.6.2 or the ICM 5.0(0) registry key tree onto the new logger.

Step 12 Run ICM *setup.exe* on the new logger (from the media, not from local setup).

Step 13 **Edit** the **Instance** and the ***component*** , insert the ***new domain name***.

Note While you can use the DNS style domain name (i.e., name.com, name.net) for Active Directory, ICM only supports a NetBIOS name (i.e., name).

Step 14 **Edit** the **Logger** component, making any necessary changes based on the new environment.

Step 15 **Exit**, then rerun ***setup.exe***.

Step 16 Run **Upgrade All**.

Note If you get an error message indicating that not all files were completely flushed, click **Continue**.

Step 17 **Reboot**.

Note When upgrading the first logger (side A) proceed to Step 18. When upgrading the second logger (side B) , skip Step 18 and proceed to Step 19.

Step 18 The first logger (side A) upgrade is complete. Proceed to *Domain Conversion Tool* and enter the information for the new environment.

Step 19 Run **ICMDBA**.

Step 20 Force the synchronization of the first logger (side A) database with the second logger (side B) database.

a. Highlight the Logger A database, then select **Main > Data/Synchronize**.

b. Identify the target server (sideB) and the database, click **Synchronize**.

c. Click **Start**, the following message appears within a few moments:

Do you really want to replace configuration of database ***<database name>*** *on Server* ***<Server name>****?*

d. Click **Yes**.

e. Click **OK** to acknowledge the successful synchronization message.

Step 21 Start up the second (side B) Logger and CallRouter. The second logger (side B) upgrade is complete. Proceed to AW Technology Refresh upgrade to continue the upgrade migration.

Domain Conversion Tool

The Domain Conversion Tool must be run on both the ICM 4.6.2 or ICM 5.0(0) and the ICM 6.0 Loggers. Copy the *DomainConversionUtility* from the *ICM Third Party CD* to the root directories of each Logger.

How to run the Domain Conversion Tool for ICM 4.6.2 or ICM 5.0(0)

Step 1 Open a command prompt on the Logger.

Step 2 Change directory to the *DomainConversionUtility* directory then run *domcvt.exe*. For example:

a. At the prompt type: **cd\DomainConversionUtility\domcvt**

b. Press **Enter**. An explanation of the options available for use in the command string appears.

Step 3 Run the Domain Conversion Tool to save user information from the Logger and domain controller into a file you specify. For example:

a. You create the directory *E:\ConversionBackup*.

b. At the prompt type: **domcvt.exe /DB:**<*enter the database name*> **/F:"E:\ConversionBackup\dbname.cvt" /M:E**

Note The location in the command string must be enclosed in double quotes.

c. A log is generated and stored in the local *DomainConversionUtility* directory.

Step 4 Verify the file has been created in the location you specified.

How to run the Domain Conversion Tool for ICM/IP Call Center Enterprise Edition, Release 6.0(0)

Note Run the Domain Conversion Tool on the ICM/IP Call Center Enterprise Edition, Release 6.0(0) Logger after *setup* is complete and the system has been rebooted.

Step 1 Open a command prompt on the Logger.

Step 2 Change directory to the *DomainConversionUtility* directory then run *domcvt.exe*. For example:

a. At the prompt type: **cd\DomainConversionTool\domcvt**

b. Press **Enter**. An explanation of the options available for use in the command string appears.

Step 3 Run the Domain Conversion Tool to move user information from the ICM 4.6.2 or ICM 5.0(0) Logger and domain controller into the new ICM/IP Call Center Enterprise Edition, Release 6.0(0) environment. For example:

Note You must be able to access the location of original ICM 4.6.2 or ICM 5.0(0) file created by the Domain Conversion Tool.

a. Access the directory *E:\ConversionBackup*.

b. At the prompt type:

domcvt.exe /DB:<*enter the database name*>
/F:"E:\ConversionBackup\dbname.cvt" /M:C /OD:<*enter the old domain name*> ***/ND:***<*enter the new domain name*> ***/P:***<*enter the password*>

Note Ensure you leave a space prior to each switch (*"space"* /M:C, *"space"*/OD:, *"space"*/ND:, *"space"*/P) in the command above.

Note Using the **/P** switch at the end of the string creates a global password for all users. If you do not use the **/P** switch, you loose your password until a new password is assigned. Be aware, this occurs globally and constitutes a security risk.

c. A log and report are generated and stored in a local *DomainConversionUtility* directory.

CallRouter Technology Refresh upgrade

How to Technology Refresh upgrade the CallRouter

Step 1 Install Windows 2000 SP4.

Step 2 Join the domain.

Step 3 Export the ICM 4.6.2 or ICM 5.0(0) registry key tree from the production CallRouter.

Step 4 Import the ICM 4.6.2 or ICM 5.0(0) registry key tree onto the new CallRouter.

Step 5 Run ICM *setup.exe* on the new CallRouter.

Step 6 **Edit** the **Instance** and the **CallRouter** component, making any necessary changes based on the new environment.

Step 7 Exit, then rerun *setup.exe*.

Note While you can use the DNS style domain name (i.e., name.com, name.net) for Active Directory, ICM only supports a NetBIOS name (i.e., name).

Step 8 Run **Upgrade All**.

CallRouter upgrade is complete.

AW Technology Refresh upgrade

How to Technology Refresh upgrade the AW

Note If installing WebView on the AW, **you must install IIS with Active Server Pages and Third Party Tools prior to running ICM *setup.exe* for the first time**. If IIS with Active Server Pages and Third Party Tools are not installed first, the AW will have to be completely rebuilt.

Step 1 Install Windows 2000 SP4.

Step 2 Join the domain.

Step 3 Install MS SQL Server 7.0 SP4 or SQL Server 2000 SP3a.

Step 4 Install IIS with Active Server Pages (ASP).

Step 5 Install Third Party Tools for WebView support.

Step 6 If custom templates exist:

a. Create a backup of the WebView database (**wvdb)** (ICM 5.0(0) only.)

b. *\userdata* directory:

- On an ICM 5.0(0) system, it is empty.
- On an ICM 4.6.2 system, it contains user created reports.

c. *\aw\custom* directory: contains the ICM 4.6.2 or ICM 5.0(0) custom templates

d. Copy the following directories from the old system onto the new system where WebView is installed.

- *icm\instancename\aw\custom* for custom templates
- *icm\instancename\dis\web\userdata* for saved reports (ICM 4,6,2 only)

e. Restore the ICM 5.0(0) **wvdb** to the new system using the MS SQL backup/restore process.

f. Create a backup of the database.

g. Restore the ICM 4.6.2 or ICM 5.0(0) AW database (**awdb**) to the new system using the MS SQL backup/restore process.

Step 7 Create the **awdb** and **wvdb** databases.

a. Open **MS SQL Enterprise Manager** on the new system.

b. Expand **Microsoft SQL Servers** and **SQL Server Group**.

c. Expand your current ***server name***.

d. Highlight **Databases**.

e. Right-click and select **New Database**.

f. Enter the new ***database name*** and set the initial ***database size*** in MB.

Note The size depends upon the size of the existing database on the old hardware.

g. Click the **Transaction Log** tab and enter the initial log size in MB.

Note The size depends upon the size of the existing log on the old hardware.

h. Click **OK**.

Step 8 Export the ICM 4.6.2 or ICM 5.0(0) registry key tree from the production AW.

Step 9 Import the ICM 4.6.2 or ICM 5.0(0) registry key tree onto the new AW.

Step 10 Run ICM *setup.exe* on the new AW .

Step 11 **Edit** the ***Instance*** and ***AW*** components, making any necessary changes based on the new environment (i.e., machine name, domain name).

Note For WebView users, while editing the AW componment, ensure WebView reporting is selected.

Note The database location is initially blank. Provide the new database location.

Note While you can use the DNS style domain name (i.e., name.com, name.net) for Active Directory, ICM only supports a NetBIOS name (i.e., name).

Step 12 Exit, then re-run *setup.exe*.

Step 13 Run **Upgrade All**.

Step 14 **Reboot**.

AW upgrade is complete.

HDS Technology Refresh upgrade

How to Technology Refresh upgrade the HDS

Note If installing WebView on the HDS, **you must install IIS with Active Server Pages and Third Party Tools prior to running ICM *setup.exe* for the first time**. If IIS with Active Server Pages and Third Party Tools are not installed first, the AW will have to be completely rebuilt.

Step 1 Install Windows 2000 SP4.

Step 2 Join the domain.

Step 3 Install MS SQL Server 7.0 SP4 or SQL Server 2000 SP3a.

Step 4 Install IIS with Active Server Pages (ASP).

Step 5 Install Third Party Tools for WebView support.

Step 6 Create a MS SQL Server backup of the production HDS database.

Step 7 IIf custom templates exist:

a. Create a backup of the WebView database (**wvdb)** (ICM 5.0(0) only.)

b. *userdata* directory:

- On an ICM 5.0(0) system, it is empty.
- On an ICM 4.6.2 system, it contains user created reports.

c. *aw\custom* directory: contains the ICM 4.6.2 or ICM 5.0(0) custom templates

d. Copy the following directories from the old system onto the new system where WebView is installed.

- *icm\instancename\aw\custom* for custom templates
- *icm\instancename\dis\web\userdata* for saved reports (ICM 4,6,2 only)

e. Restore the ICM 5.0(0) **wvdb** to the new system using the MS SQL backup/restore process.

f. Create a backup of the database.

g. Restore the ICM 4.6.2 or ICM 5.0(0) AW database (**awdb**) to the new system using the MS SQL backup/restore process.

Step 8 Create the **HDS**, **AW** and **WebView** databases.

a. Open **MS SQL Enterprise Manager** on the new system.

b. Expand **Microsoft SQL Servers** and **SQL Server Group**.

c. Expand your current ***server name***.

d. Highlight **Databases**.

e. Right-click and select **New Database**.

f. Enter the new ***database name*** and set the initial ***database size*** in MB.

Note The size depends upon the size of the existing database on the old hardware.

g. Click the **Transaction Log** tab and enter the initial log size in MB.

Note The size depends upon the size of the existing log on the old hardware.

h. Click **OK**.

Step 9 Restore the MS SQL Server backup onto the new HDS using the MS SQL backup/restore process.

Step 10 Export the appropriate ICM file/folders tree from the production HDS.

Step 11 Export the ICM 4.6.2 or ICM 5.0(0) registry key tree from the production HDS.

Step 12 Import the ICM 4.6.2 or ICM 5.0(0) registry key tree onto the new HDS.

Step 13 Run ICM *setup.exe* on the new HDS (from the media, not from local setup).

Step 14 **Edit** the ***Instance*** and ***HDS/AW*** components, making any necessary changes based on the new environment.

Note For WebView users, while editing the AW componment, ensure WebView reporting is selected.

Note While you can use the DNS style domain name (i.e., name.com, name.net) for Active Directory, ICM only supports a NetBIOS name (i.e., name).

Step 15 Exit, then re-run *setup.exe*.

Step 16 Run **Upgrade All**.

Step 17 **Reboot**.

HDS upgrade is complete.

All other component Technology Refresh upgrades (PG included)

How to Technology Refresh upgrade all other components (PG included)

Step 1 Install Windows 2000 SP4.

Step 2 Join the domain.

Step 3 Export the ICM 4.6.2 or ICM 5.0(0) registry key tree from the production component.

Step 4 Import the ICM 4.6.2 or ICM 5.0(0) registry key tree onto the new component.

Step 5 Run ICM *setup.exe* on the new component.

Step 6 **Edit** the ***Instance*** and ***<component>***, making any necessary changes based on the new environment.

Note While you can use the DNS style domain name (i.e., name.com, name.net) for Active Directory, ICM only supports a NetBIOS name (i.e., name).

Step 7 Exit, then re-run *setup.exe*.

Step 8 Run **Upgrade All**.

Step 9 **Reboot**.

Other component upgrade migration is complete.

CHAPTER 12

ICM 4.6.2 or ICM 5.0(0) to ICM/IP Contact Center Enterprise Edition, Release 6.0(0) SQL Server Installation and Upgrade

Overview

This topic covers both installing SQL Server 2000 (for technology refresh upgrades) and upgrading SQL Server 7.0 to SQL Server 2000 (for common ground upgrades) in the Cisco ICM environment.

Installing MS SQL Server 2000

Installing MS SQL Server 2000 on the new system acts as your upgrade when performing technology refresh upgrade migrations. SQL Server 2000 can be installed on either Windows NT or Windows 2000 Server.

ICM 5.0 (0) and ICM/IP Contact Center Enterprise Edition, Release 6.0(0) support SQL Server 2000 and require Windows 2000 Server as their running environment to support all ICM 5.0(0) and ICM/IP Contact Center Enterprise Edition, Release 6.0(0) features.

SQL Server 2000 *Standard Edition* is supported by ICM 5.0(0) and ICM/IP Contact Center Enterprise Edition, Release 6.0(0).

Refer to How to install SQL Server 2000 and How to create ICM databases for detailed information.

How to install SQL Server 2000

Step 1 Select *SQL Server 2000 Standard Edition* to start SQL Server setup.

Step 2 On the first screen:

a. Select **Install SQL 2000 Server Components**.

b. Select **Install Database Server**.

c. Read the *Welcome* screen.

d. Click **Next**.

Step 3 On the *Computer Name* screen:

a. Choose the default, **Local Computer**.

b. Click **Next**.

Step 4 On the *Installation Selection* screen:

a. Choose the default, **Create a new instance of SQL Server**.

Optionally, install **Client Tools**. (This upgrade option is available only when SQL 7.0 exists on the machine).

b. Click **Next**.

Step 5 On the *User Information* screen:

a. Enter the **user name** and **company name**.

b. Click **Next**.

Step 6 On the *Software License Agreement* screen:

a. Read the terms of the license agreement, then click **Yes**.

Step 7 On the *Installation Definition* screen:

a. Choose the default **Server and Client Tools**.

b. Click **Next**.

Step 8 On the next screen:

a. For *Instance Name*, check **Default**.

b. Click **Next**.

Step 9 On the *Setup Type* screen (see Figure 2):

a. Select **Custom** for the setup type.

b. Install the program files to any disk with space available (default is C:)

Note MS SQL disk space requirements: 270MB (full installation), 250MB (typical), 95MB (minimum), 44 MB (Desktop Engine) plus Analysis Services: 50 MB minimum and 130 MB typical and 80 MB for the English Query. Check your MS SQL documentation for additional information.

Step 10 On the *Select Components* screen:

a. Uncheck **Install Books Online**.

b. Leave all other fields set to their **default values**.

c. Click **Next**

Step 11 Under *Services Accounts* select items in exactly this order:

a. Customize settings for each service.

b. Select **Use local system account** (SQL Server is already selected).

c. Check **Auto-start service**.

d. Select **SQL Server Agent**.

e. Select **Use local system account**.

f. Check **Auto-start service**.

g. Click **Next**.

Note A pop-up dialog explaining a dependency appears, click **OK**.

Step 12 On the *Collation Settings* screen:

a. *S*et *Collation Designer* to **Latin1_General**.

b. Set the *Sort Order* to **Binary**.

c. Leave other files set to their **default values**.

d. Click **Next**.

Step 13 Under *Network Libraries*:

a. Uncheck all choices except for **Named Pipes** unless instructed otherwise.

Step 14 On the *Start Copying Files* screen:

a. Read and click **Next**.

Step 15 On the next screen:

a. Select **Per Seat** as the *Licensing method*.

b. Set at least **40 devices** to prevent running out of licenses for database connections.

Note If you need to choose *Processor License* for licensing reasons, make sure there are sufficient concurrent connection licenses so that the system will not run into licensing problems. There should be at least 40 concurrent connections, though the precise number depends on the accessing need.

Step 16 A dialog box with the message *Setup is installing Microsoft Data Accessing Components (MDAC) ...* appears.

Note Occasionally, MDAC installation fails. The remedy is to download MDAC 2.7, or later, from a Microsoft website and install it. Once MDAC has been installed, run SQL Server setup again.

Note If a message box for *Configure SQL Server Agent* pops up, click **OK**.

The SQL 2000 installation is now complete.

Once SQL server 2000 is installed, install the appropriate service pack(s). Refer to How to install SQL Server service packs for additional information.

When the appropriate SQL Server 2000 service pack is installed, create the ICM database and adjust the database setting. Refer to How to create ICM databases for additional information.

Installing SQL Server service packs

SQL Server service packs can be obtained by accessing the Microsoft web site.

How to install SQL Server service packs

Step 1 Download the appropriate SQL Server service pack. (SQL Server 2000 SP3a in this case.)

Step 2 Following the instructions provided with the service pack, install it.

Creating ICM Databases

How to create ICM databases

Step 1 When SQL Server setup and service pack installation is complete, reboot the server.

Step 2 Install the applicable ICM component(s) (Logger, RTD, AW, HDS, etc.) and hot fixes.

a. Refer to the applicable node forms, checklists, and technical documentation for installing ICM software.

Step 3 Verify that SQL Server is running.

Step 4 Select **Start > Run > icmdba**. Use *ICMDBA* to create the appropriate database(s). Directions on how to use this tool can be found in the 5.0 *Cisco ICM Software Administrator Guide*.

You may be prompted that the following items need to be changed:

- Set the *TempDB Size* to at least **100 MB**, then click **OK**.
- Set the *TempDB Log* to at least **20 MB**, then click **OK**.

a. If the local server is not listed, create it by selecting **File > Add Server**

b. Enter the **local server name**.

c. Drill down to the server you are working on.

d. Select the server.

e. Add the data devices by highlighting the disk drive in the device field.

f. Enter the size of the database device.

g. Add the appropriate Log Devices. The size of this device typically should not be larger than 500 MB for most ICM installations.

h. Enable partitioning if applicable.

i. Click **Database > Create**.

Note The amount of time necessary to create the database is dependant on the database size.

Once the database is created, configure SQL Server 2000.

How to configure SQL Server

Step 1 Select **Start > Programs > Microsoft SQL Server > Enterprise Manager**.

Step 2 Right click on each DB and select **Properties.** Check the properties of each database in Enterprise manager (the ICM database, the temp database, and the master database).

a. Click on Data Files tag.

b. Set the database size large enough to be sufficient for the foreseeable future if disk space is available.

c. Enable **Automatically grow file**.

d. Set *Automatically grow by percent* to **10%**.

e. Set the *Maximum file size* to **Restrict file growth**. Database file growth is obviously limited by the physical disk space available. It is up to you to set the a suitable maximum size.

Note Setting maximum file size is important because database file growth may potentially use all the disk space and can cause system-wide problems. If the database files are on the system disk (for example C:), it is recommended that the size of all database files should not be over 80% of all the disk space because running out of disk space on the system disk is not a desirable scenario. It is also important to remember that there can be many databases on a single database server and many disk files on a single disk. Each data file should only use its share of disk to avoid running out of disk space. This setting is based on your configuration and is up to you to do the calculation for the limits.

f. Verify correct sizing of each database.

Databases include: ICM logger DB, AW DB, or HDS DB (depending on ICM node)

tempdb should be at least **100 MB**

master db should be at least **50 MB**

g. Verify correct sizing of the *transaction log* for each database.

Databases include: ICM logger DB, AW DB, or HDS DB (depending on ICM node)

Under the *transaction log tab* for each database, **disable auto-grow**.

Note It is recommended that transaction log in ICM system to be kept under 500M to allow rapid recovery in case of restarting the system. Even though the database files are allowed to automatically grow, the size of the transaction log growth should be changed manually.

ICM logger DB, AW DB, or HDS DB transaction log (depending on ICM node).

tempdblog should be at least **20 MB**

master db log should be at least **20 MB**

h. Do not change anything under the *Permissions tab.*

i. Select the *Options tab* and set the options as follows:

ANSI NULL default: **No**

Recursive triggers: **No**

Auto update statistics: **Yes**

Torn page detection: **Yes**

Auto close: **No**

Auto shrink: **No**

Auto create statistics: **Yes**

Use quoted identifier: **No**

All other parameters should be left as default

Step 3 If changes are needed, the MSSQLSERVER Service may need to be cycled.

Step 4 Close SQL Enterprise Manager.

Pre-Upgrade database planning

To upgrade from SQL Server 7.0 to SQL Server 2000, there is not much planning to do because there is no data transfer of during the upgrade.

Upgrading MS SQL Server 7.0 to MS SQL Server 2000

The SQL Server 7.0 to SQL Server 2000 upgrade is used during a common ground upgrade migration.

How to upgrade SQL Server 7.0 to SQL Server 2000

Step 1 Copy the *SQL Server 2000 Installation CD* to a disk.

Step 2 Using the MS SQL Backup/Restore procedure, back up all databases to be upgraded.

Note Backing up the *cust_awdb* is not required.

Step 3 Using the ICM service control, stop all ICM services on the local server.

Step 4 Make sure no one is using SQL Server 7.0 as the upgrade process turns off the server.

a. To identify any active SQL users, run the SQL query ***sp-who2***.

Step 5 Start SQL Server 2000 *autorun.exe*.

Step 6 On the first screen:

a. Select **Install SQL 2000 Server Components**.

b. Select **Install Database Server**.

Step 7 Read the *Welcome* screen, then click **Next**.

Step 8 On the *Computer Name* screen:

a. Make sure the default of **Local Computer** is selected and the correct server name is present.

b. Click **Next**.

Step 9 On the *Installation Selection* screen:

a. Choose **Upgrade, remove, or add components to an existing instance of SQL Server**.

b. Click **Next**.

Step 10 On the *Instance Name* screen:

a. Make sure **Default** is checked.

b. Click **Next**.

Step 11 On the *Existing Installation* screen:

a. Select **Upgrade your existing installation**.

b. Click **Next**.

Step 12 On the *Upgrade* screen:

a. Check **Yes, upgrade my SQL Server Tools and data**.

b. Click **Next**.

Step 13 On the *Connect To Server* screen:

a. Select **Windows Authentication**.

b. Click **Next**.

Step 14 Read the *Start Copying Files* screen, then click **Next**.

Step 15 On the *Licensing* screen, in the *Choose License Mode* section:

a. Set the licensing method to **per seat.**

b. Set at least **40** devices.

c. Click **Continue**.

Note If you need to choose Processor License for licensing reasons, make sure there are sufficient concurrent connection licenses to ensure the system does not run into licensing problems. While the precise number depends on the accessing need, there should be at least 40 concurrent connections.

Note MS SQL may display an MDAC 2.6 setup screen indicating tasks (for example, Jaguar, SNMP) that must be shut off in order to proceed. Make a note of the services you stop as they may not restart after the upgrade is complete.

Step 16 If the *Setup is installing Microsoft Data Access Components* screen is shown, click **Finish.**

The installation is now complete.

The SQL Server 2000 installation is now complete.

Once SQL server 2000 is installed, install the appropriate service pack(s). Refer to How to install SQL Server service packs for additional information.

How to re-establish NT authentication between ICM and MS SQl Server

Step 1 Run ICM *setup.exe*.

a. In a command window type: **c:\icm\bin** and press **Enter**.

b. Type **setup** and press **Enter**.

c. Click **Upgrade All**.

d. Click **Finish**.

Step 2 Start the upgraded machine.

Step 3 Verify there are no ICM process errors and no SQL error log.

System Integrity Tests

The purpose of the sample test cases in this appendix is to validate basic ICM functionality and fault tolerance prior to, during and after each step of the upgrade migration project.

Table A-1 System Integrity Test 1 – Zero ICM Process Errors

Test Number:	**1**
Test Title:	**Validation of ICM Processes**
Test Purpose:	**Verify that the ICM Processes have no errors**
Test Setup:	**All ICM Services are started**
Procedure:	**1. Visually check key ICM process windows**
Expected Results:	
1. Call Routers • Router: UP and synchronized with peer (unless running in simplex) • Ccagent: connected to all configured peripheral gateways • Rtsvr: feed activated to AW • NIC Online (if one configured)	**Pass: __ Fail: __**

2. Loggers • Logger: connected to its respective database and synchronized with peer (unless running in simplex) • MDS is inservice • If HDS - Replication: connected to AW	**Pass: __ Fail: __**
3. Admin Workstation • Updateaw: displays “waiting for new work” • If HDS - Replication: replication and recovery client connection initialized	**Pass: __ Fail: __**
4. Peripheral Gateways • Mdsproc: inservice • Pgagent: inservice and active to one side of central controller • PIM’s: ACTIVE	**Pass: __ Fail: __**
5. CTI Server • Cg[#]ctisvr: active with configured port number	**Pass: __ Fail: __**
Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

Table A-2 System Integrity Test 2 - RTTEST

Test Number:	**2**
Test Title:	**RTTEST**

Test Purpose:	**Verify the current state of all ICM Central Site Processes and that all devices (PG's and Peripherals) are identified correctly by the CallRouter.**
Test Setup:	**All ICM Services are started in full Duplex Mode (unless running in simplex) – Run RTTEST on each CallRouter**
Procedure:	**1. Run: Rttest /system <CallRouterHostname> /cust <instance name> /node routera** **2. RTTEST: status** **3. Take a screen shot of results and append to Staging Report** **4. Quit to exit out of command prompt when finished on each CallRouter**

Expected Results:	
1. All configured processes are OK as seen by CallRouter	**Pass: __ Fail: __**
2. All configured physical controllers are communicating (CFO) with CallRouter	**Pass: __ Fail: __**
3. All configured/in-service Peripherals are properly identified by that CallRouter and are online	**Pass: __ Fail: __**

Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

Table A-3 System Integrity Test 3 – RTTEST debug/route

Test Number:	**3**
Test Title:	**RTTEST debug/route**
Test Purpose:	**Verify that all calls are being sent to the ICM router and labels are being generated back tot eh NIC.**
Test Setup:	**All ICM Services are started in full Duplex Mode (unless running in simplex)– Run RTTEST on each CallRouter**

Procedure:	1. Run: Rttest /system <CallRouterHostname> /cust <instance name> /node routera 2. RTTEST: status 3. Type: debug/route 4. Dump the router process log 5. Review log for text similar to the following example: **15:21:39 ra-rtr Trace: Route: dn=8004284322 ani=4127475709 ced=1 label=1684734757** **15:21:39 ra-rtr Trace: Route: CRSDateOfCall=145679 CRSCallKey=105821** **15:22:14 ra-rtr Trace: Route: dn=8886387653 ani=4403568854 ced= label=1620000006** **15:22:14 ra-rtr Trace: Route: CRSDateOfCall=145679 CRSCallKey=114359**

Expected Results:	
1. Router log shows similar data output to example above.	**Pass: __ Fail: __**
2. Calls are observed routing to the proper target.	**Pass: __ Fail: __**

Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

Table A-4 System Integrity Test 5 – SQL errorlog Review

Test Number:	**5**
Test Title:	**SQL errorlog Review**
Test Purpose:	**Verify the SQL errorlogs on the upgraded logger shows proper functionality and no errors.**
Test Setup:	**All ICM Services are started on upgraded logger – dump the SQL errorlog**
Procedure:	**1.** Go to c:\mssql7\log **2.** Type: type errorlog **3.** Review SQL errorlog

Expected Results:	
1. Errorlog should show “Recovery Completed”.	**Pass: __ Fail: __**
2. Errorlog should show proper SQL version.	**Pass: __ Fail: __**
3. No errors should be observed.	**Pass: __ Fail: __**

Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

Table A-5 System Integrity Test 6 - OPCTEST

Test Number:	**6**
Test Title:	**OPCTEST**
Test Purpose:	**Verify connectivity of pgagent and PIM processes on each logical PG pair**
Test Setup:	**All ICM Services are started in full Duplex Mode (unless running in simplex)**
Procedure:	**1.** Run: opctest /cust <instance name> /node <logical pg node number/side> **2.** opctest: status **3.** Take a screen shot of results and append to Staging Report **4.** Quit to exit out of command prompt when finished on each PG

Expected Results:	
1. Active PGAgent is CONNECTED to both sides of central controller (unless running in simplex)	**Pass: __ Fail: __**
2. Associated PIM's are Active on one of the PG pair	**Pass: __ Fail: __**
3. CTI Server is Active on one of the PG pair	**Pass: __ Fail: __**

Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

Table A-6 System Integrity Test 7 – Central Controller Fault Tolerance

Test Number:	**7**
Test Title:	**Central Controller Fault Tolerance**
Test Purpose:	**Verify that Central Controllers function in Simplex Mode**
Test Setup:	**All ICM Services are started in full Duplex Mode**
Procedure:	**1.** Stop Router Service on CallRouter A **2.** On CallRouter B, open Router process and check for messages that indicate Router A processes are down **3.** Start Router Service on CallRouter A **4.** On Router B check for messages that indicate that CallRouter A Router and Logger processes are now OK **5.** Repeat steps 1-4 stopping Router B and validating Simplex Mode on Router A

Expected Results:	
1. CallRouter B will indicate that Side A Central Site is DOWN when Router Service is stopped on CallRouter A	**Pass:** __ **Fail:** __
2. CallRouter B will indicate that it is syncrhonized with CallRouter A when Router Service is started on CallRouterA	**Pass:** __ **Fail:** __
3. Call Router B will indicate that Side A Router and Logger Processes are OK when Router Service is started on CallRouterA	**Pass:** __ **Fail:** __
4. CallRouter A will indicate that Side B Central Site is DOWN when Router Service is stopped on CallRouter B	**Pass:** __ **Fail:** __
5. CallRouter A will indicate that it is syncrhonized with CallRouter B when Router Service is started on CallRouterB	**Pass:** __ **Fail:** __
6. Call Router A will indicate that Side B Router and Logger Processes are OK when Router Service is started on CallRouterB	**Pass:** __ **Fail:** __

7. Call Processing functions as designed when Routers are in Simplex Mode.	**Pass: __ Fail: __**
Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

Table A-7 System Integrity Test 8 - PG Fault Tolerance

Test Number:	**8**
Test Title:	**PG Fault Tolerance (create a test case for each logical PG pair)**
Test Purpose:	**Verify that PG's communicate with Central Controller in Simplex Mode and that PIM's remain active**
Test Setup:	**All PG Services are started in Duplex Mode**
Procedure:	**1.** Verify that PGA is Active **2.** Verify that PGB is Idle **3.** Stop Service on PGA **4.** Observe PGB change of state from Idle to Active **5.** Start Service on PGA **6.** Observe PGA state as Idle **7.** Repeat Steps 1-6 stopping PGB to validate PG failover to PGA

Expected Results:	
1. B Side PG will maintain connectivity to the Central Contoller and the PIM will be Active	**Pass:** __ **Fail:** __
2. Upon Restart of A side PG, A side MDS/OPC processes will note the state change to Idle while B Side PG remains Active	**Pass:** __ **Fail:** __
3. A Side PG will maintain connectivity to the Central Contoller and the PIM will be Active	**Pass:** __ **Fail:** __

Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

Table A-8 System Integrity Test96 - AW Configuration and Scripting Tools

Test Number:	**9**
Test Title:	**AW Tools**
Test Purpose:	**Validate basic configuration and scripting functionality of ICM**
Test Setup:	**All Router, Logger, AW services are started**
Procedure:	**1.** Configure ICM: For Call Manager Routing Client, Add Dialed Number of 5555, Label of 1111 and Call Type named stagingtest **2.** Create routing script named stagingtest wherein DN of 5555 returns label of 1111. Schedule call type for all day/every day and associate stagingtest script with stagingtest call type **3.** Place script named stagingtest in monitor mode **4.** Run Call Tracer for Call Manager Routing Client with DN of 5555

Expected Results:	
1. Configuration and Script are created and saved with no error messages from ICM tools	**Pass: __ Fail: __**
2. Call Tracer returns expected label of 1111	**Pass: __ Fail: __**

Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

Table A-9 System Integrity Test 10 - Webview

Test Number:	**10**
Test Title:	**Webview**
Test Purpose:	**Webview Reporting Tool opens and is navigable by authorized ICM user**
Test Setup:	**All Router, Logger, AW Services started**
Procedure:	**1.** 1. Create Webview User via Configure ICM\Security\User List • Domain Name – example: CUS • User Name – example: test1 • Password – example: test1 • Check "can create other user accounts" **2.** Open and Login to Webview • Open Browser and enter URL: http: //<AW hostname>/<icm instance name> • Enter User Name: <AW domain name>/<user name from ICM User List> **Note** Note: the user name in Webview is case sensitive • Enter Password: <password associated with user name> **3.** Select Webview Reports **4.** Select various reports from left hand panel

Expected Results:	
1. New User successfully created in ICM	**Pass: __ Fail: __**
2. New User can login to Webview	**Pass: __ Fail: __**
3. New User can open report categories and access all report templates	**Pass: __ Fail: __**
Passed: (initial)	
Failed: (initial)	

Reason for Failure:	
Remarks:	

Table A-10 System Integrity Test 11 - Internet Script Editor

Test Number:	**11**
Test Title:	**Internet Script Editor**
Test Purpose:	**Webview Reporting Tool opens and is navigable by authorized ICM user**
Test Setup:	**All Router, Logger, AW Services started**
Procedure:	**1.** Create ISE User via Configure ICM\Security\User List • Domain Name – example: CUS • User Name – example: test2 • Password – example: test2 • Check "can create other user accounts" **2.** Install ISE Client on Desktop • URL: <AW IP Address>\install\iscripteditor.htm – enter • Click on ISE download link – save to desktop - when download complete, close browser • open iscripteditor.exe which is now on desktop– complete ISE installation (shortcut will be on desktop) **3.** 3. Establish ISE Connection • Open ISE Client • In Connection Window, enter address, port (defaults to 80), instance name – OK • Enter username, password and domain name of Admin Workstation **4.** Open script named stagingtest, place in edit mode, change position of DN node, save script

Expected Results:	
1. ISE Client is downloaded successfully to desktop	**Pass: __ Fail: __**
2. ISE Client accesses Script Editor on AW	**Pass: __ Fail: __**
3. User can open, edit and save script	**Pass: __ Fail: __**

Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

Table A-11 System Integrity Test 12 - Review of Setup.log file

Test Number:	**12**
Test Title:	**Review of Setup.log file**
Test Purpose:	**Review setup.log file for errors during the upgrade**
Test Setup:	**This file in the c:\temp directory on every ICM node**
Procedure:	**1.** Go to c:\temp\setup.log in a command line. **2.** Type "findstr –I error setup.log" **3.** Type "findstr –I fail setup.log"
Expected Results:	
No errors or failures should exist in this log file.	**Pass: __ Fail: __**
Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

Table A-12 System Integrity Test 13 - Review of .log files

Test Number:	**13**
Test Title:	**Review of .log files**
Test Purpose:	**Review icmsetup.log and apply.log file for errors during hotfix installation.**
Test Setup:	**This file in the c:\icr directory on every ICM node**
Procedure:	**1.** Go to c:\icr\apply.log and c:\temp\icmsetup.log in a command line. **2.** Type “findstr –I error install.log” **3.** Type “findstr –I fail install.log”
Expected Results:	
No errors or failures should exist in this log file.	**Pass: __ Fail: __**
Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

APPENDIX B

Post-Migration Application Tests

This section details the tests necessary to confirm the functionality of the application configuration. It is the customer's responsibility to create, run and record all Post-Migration Application Tests. Tests are broken down by component. Each component test explains the necessary system prerequisites, test procedures and expected results with a pass/fail determination.

Table B-1 [example test format]

Test Number:	**<#>**	
Test Title:		
Test Purpose:		
Test Setup:		
Procedure:		
Expected Results:		
1.		**Pass: Fail:**
2.		**Pass: Fail:**
3.		**Pass: Fail:**

Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

A

Auto Attendant 1-2, 3-2
AW Forklift upgrade 6-6, 11-12
AW real time client
  software requirements 4-3, 9-4
AW real time distributor/WebView server
  software requirements 4-3, 9-3

B

baseline
  definition 4-1, 9-2
bill of material 1-2, 3-1, 4-2, 8-1, 9-3
BOM 1-2, 3-1, 4-2, 8-1, 9-3

C

CAD 8-2
Call Manager 1-2, 3-1
CallManager 8-2
CallRouter
  software requirements 4-2, 9-3
CallRouter Forklift upgrade 6-3, 11-12
Cisco Agent Desktop 8-2
Common Ground upgrade
  Key AWs 5-3
Common Ground Upgrade Migration
  MS SQL Server upgrade 5-5
common ground upgrade migration 1-2, 3-1, 8-1
configuration updates 5-7, 5-17, 10-26
CRA
  IP IVR 8-2
CTI desktop/client 1-2, 3-1
CTI OS 8-2

D

data backup plan 2-1, 2-3, 4-1, 9-1
default routing plan 2-1, 4-1, 9-1
disabling 5-7
Domain Conversion Tool 6-5, 11-10

E

enabling 5-17, 10-26

F

Forklift upgrade

AW 6-6
CallRouter 6-3, 11-12
HDS 6-7, 11-15
Logger 6-3, 11-7
PG 6-9, 11-17
forklift upgrade migration 1-2, 3-1

G

Go/No Go decision 5-9

H

hardware recommendations 4-2, 9-2
HDS Forklift upgrade 6-7, 11-15
how to
backup the AW HDS database if the machine is a Historical Data Server 5-10
back up the ICM directory 2-4
configure SQL Server 7-8, 12-6
create ICM databases 7-5, 12-5
disable configuration changes 5-7, 5-10, 10-18
enable configuration changes 5-17, 10-26
enable configuration updates 5-22, 10-32
Forklift upgrade all other components (PG included) 6-9, 11-17
Forklift upgrade the AW 6-6
forklift upgrade the CallRouter 6-3, 11-12
forklift upgrade the HDS 6-7
forklift upgrade the Logger 6-3, 11-7
install SQL Server 2000 7-2, 12-2
install SQL Server service packs 7-5, 12-5
make the Go/No Go decision to upgrade ICM side B 5-17, 10-26
run the Domain Conversion Tool for 4.6.2 6-5
run the Domain Conversion Tool for 5.0 6-5
run the Domain Conversion Tool for ICM/IP Call Center Enterprise Edition, Release 6.0(0) 11-10
run the Domain Conversion Tool for ICM 4.6.2 11-10
run the Domain Conversion Tool for ICM 5.0(0) 11-10
start ICM side A and the Key AW 10-25
start ICM side A and the Key AW(s) 5-16
start ICM side B 5-20, 10-30
stop ICM side A 5-12, 10-21
stop ICM side B 5-15
stop ICM side B and remaining AWs 10-25
Technology Refresh upgrade the AW 11-12
Technology Refresh upgrade the HDS 11-15
upgrade SQL Server 7.0 to SQL Server 2000 7-7, 12-8
upgrade the ICM side A Central Controller 5-14, 5-19, 10-23, 10-28
upgrade the Key Admin Workstation(s) 5-12, 10-21
upgrade the side B Key Admin Workstation(s) 5-18, 10-27
validate default network routing 5-16, 10-25
validate ICM side A routing is restored 5-17, 10-26

I

ICM databases
  creating 7-5, 12-5
installing SQL Server 2000 7-1, 12-1
installing SQL Server service packs 7-5, 12-5
Internet Service Node 8-2
IPCC 1-2, 3-1
IPIVR 1-2, 3-1
ISN 8-2

K

Key AW Common Ground upgrade 5-3

L

logger
  software requirements 4-3, 9-3
Logger Forklift upgrade 6-3, 11-7

N

network inventory 2-1, 4-1, 9-1

P

peripheral gateway
  software requirements 4-3, 9-4
Personal Assistant 1-2, 3-2
PG
  software requirements 4-3, 9-4
PG Forklift upgrade 6-9, 11-17
post-upgrade test definition 2-1, 4-1, 9-1
Pre-upgrade Testing 2-1
pre-upgrade testing 2-1

R

recording solutions 1-2, 3-2
related publications 4-3, 9-4

S

schedule of upgrade activities 2-1, 4-1, 9-1
software requirements 4-2, 9-3
  AW real time client 4-3, 9-4
  AW real time distributor/WebView server 4-3, 9-3
  CallRouter 4-2, 9-3
  logger 4-3, 9-3
  peripheral gateway 4-3, 9-4
  PG 4-3, 9-4
SQL Server
  installation 7-1, 12-1
  upgrade 7-1, 12-1
SQL Server 2000
  how to install 7-2, 12-2

installation 7-1, 12-1
SQL Server service packs
installation 7-5, 12-5
stakeholder notification 2-6
stakeholders 2-1, 4-1, 9-1
system critical data 2-3

T

Technology Refresh upgrade
AW 11-12
Technology refresh upgrade migration 8-1
test plan 2-1, 2-4, 4-1, 9-1

U

Unity 1-2, 3-2
upgrade activities
Common Ground 5-6, 10-12
upgrade planning 2-1, 4-1, 9-1
data back up plan 2-3
data backup plan 2-1, 4-1, 9-1
default routing plan 2-1, 4-1, 9-1
definition of upgrade steps 2-1, 4-1, 9-1
network inventory 2-1, 2-2, 4-1, 9-1
post-upgrade test definition 2-1, 4-1, 9-1
pre-upgrade testing 2-1
schedule of upgrade activities 2-1, 4-1, 9-1
stakeholder notification 2-1, 4-1, 9-1
test plan 2-1, 4-1, 9-1
upgrade tests
definition of 2-1, 4-1, 9-1
Upgrading MS SQL Server
Forklift Upgrade Migration Method 6-2, 11-7
upgrading SQL Server 7.0 to SQL Server 2000 7-6, 12-8

V

validate scripts
post upgrade 10-32