Upgrade Guide
for Cisco Unified ICM/Contact Center Enterprise & Hosted

Release 7.5(1)

May 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0833

Table of Contents

List of Figures

Preface

Purpose

This document describes the procedure for upgrading a Cisco ICM/IP Contact Center Enterprise Edition, Release 7.0(x), 7.1(x), or 7.2(x) system to a Cisco ICM/IP Contact Center Enterprise Edition, Release 7.5(1) system. This document further addresses the acceptable component release compatibilities as well as their operating system and database server releases. A baseline for start of upgrade to ICM 7.5(1) is defined in this document and further addresses the acceptable component version compatibilities that are allowed during and after the upgrade process is complete.

Audience

This document is intended for both Customer and Cisco representatives (trained in Cisco ICM software system administration and troubleshooting) performing a system upgrade.

This document assumes that as a member of the Upgrade Team you meet the following skill set requirements:

- Familiar with Windows Operating System
  - Active Directory
  - Security concepts
  - Network configuration and operation
- Familiar with SQL Server
  - Enterprise Manager

  - Query Analyzer
  - SQL scripting
- ICM/IPCC knowledge
  - ICM/IPCC Nodes (CallRouter, Logger, AW, PGs)
  - HDS Schema knowledge
  - Deployment models (including WebView)
  - Have read the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html) and **Cisco Unified Contact Center Enterprise 7.5 Solution Reference Network Design (SRND)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html).

Organization

Part	Chapter	Description
Part 1: Pre-upgrade Preparation	Chapter 1: ICM/IPCC Upgrade Planning (page 11)	Discusses planning to upgrade your ICM/Contact Center system. This includes discussions of the following: • the hardware requirements • pre-upgrade testing • the data backup plan • pre-upgrade ICM server preparation • network configuration backup • the default routing plan • the test plan • a definition of upgrade steps • post-upgrade test definition • stakeholder notification • related documents

Part	Chapter	Description
Part 2: ICM/IPCC Software Upgrade	Chapter 2: Getting to the Baseline (page 21)	Discusses the baseline requirements that must be met prior to upgrading your ICM/Contact Center system.
	Chapter 3: Common Ground Upgrades vs. Technology Refresh Upgrades (page 23)	Describes the two upgrade methods and when each is used.
	Chapter 4: Introduction to ICM/IPCC Upgrade (page 25)	Provides a high-level overview of the ICM/Contact Center upgrade process.
	Chapter 5: ICM/IPCC 7.5(1) Upgrade Time and SpaceRequirements (page 29)	Discusses the time and space requirements necessary to upgrade the various ICM/Contact Center components. This includes a discussion of database migration performance; and provides time guidelines and migration performance values.
	Chapter 6: Setting Up the Hardware (page 35)	Provides the information necessary to setup your hardware prior to an upgrade. The topics include: • the hardware prerequisites for both a technology refresh and a common ground upgrade • how to set up the hardware • installing Microsoft Windows 2003 • upgrading from Windows 2000 to Windows Server 2003 • Windows 2003 hardware compatibility • Active Directory considerations for common ground upgrades • Internet Information Services (IIS) 6.0 considerations for common ground upgrades • operating system upgrade considerations for WebView • installing Microsoft SQL Server 2005

Part	Chapter	Description
		• upgrading from SQL Server 2000 to SQL Server 2005 • Support Tools considerations for upgrades • Active Directory and DNS considerations for upgrades • verifying system conditions using EDMT
	Chapter 7: Enhanced Database Migration Tool (EDMT) forICM/IPCC 7.5(1) (page 59)	Describes the Enhanced Database Migration Tool (EDMT) and how it is used to migrate the Logger and HDS database schemas to the ICM/IPCC 7.5(1) database schema.
	Chapter 8: Service Account Manager (page 79)	Describes the Service Account Manager tool and describes how to use it to manage the service accounts.
	Chapter 9: Upgrade Procedures (page 101)	Provides multiple upgrade examples and the procedures for each. It also provides high-level information concerning the ICM/IPCC component upgrade process.
	Chapter 10: Administrative Workstation (AW) Upgrade Procedures (page 115)	Provides the specific steps necessary to upgrade an AW for the following deployment types: • Distributor AWs with HDS and WebView Server (primary and secondary) • Distributor AWs with HDS without WebView Server (WebView Servers on dedicated hardware) • Distributor AWs without HDS • Client AWs
	Chapter 11: Logger Upgrade Procedures (page 133)	Provides the specific steps necessary to upgrade the logger.
	Chapter 12: CallRouter Upgrade Procedures (page 139)	Provides the specific steps necessary to upgrade the CallRouter
	Chapter 13: Peripheral Gateway (PG) Upgrade Procedures (page 147)	Provides the specific steps necessary to upgrade a PG.

Part	Chapter	Description
	Chapter 14: Network Gateway Upgrade Procedures (page 159)	Provides the specific steps necessary to upgrade the network gateway.
	Chapter 15: Upgrading a Localized ICM/IPCC System (page 163)	Provides localization considerations when upgrading your ICM/Contact Center system.
	Chapter 16: CIS Upgrade Procedures (page 165)	Provides CIS component upgrade information.
	Chapter 17: CTI OS Agent and Supervisor Desktop Upgrade Procedures (page 167)	Provides the specific steps necessary to upgrade the CTI OS Agent and Supervisor Desktops.
	Chapter 18: Cisco Agent Desktop (CAD) Upgrade Procedures (page 169)	Provides the specific steps necessary to upgrade Cisco Agent Desktop (CAD).
	Chapter 19: Remote Monitoring System (RMS) Upgrade Procedures (page 171)	Provides the specific steps necessary to upgrade the Remote Monitoring System (RMS).
	Chapter 20: Database Tasks (page 173)	Provides the specific steps necessary to perform the following database tasks: • How to create an ICM Database for the Technology Refresh Restore Process • How to set the Logger or HDS database data file size for maximum growth using SQL Enterprise Manager • How to Determine the Size of an ICM Database • How to Set the tempdb Database Size
	Chapter 21: Upgrade Checklists (page 177)	Provides upgrade checklists for TR and CG upgrades..
Part 3: Post-upgrade Testing	Chapter 22: Post-Upgrade Testing (page 191)	Discusses post-upgrade test plan development. This includes application, system integrity, process, redundancy, alarm, historical reporting, WebView reporting, and Internet Script Editor testing. In addition, this chapter discusses how to set the ICM services to automaticially start, how to run post-upgrade tests, and how to validate scripts.

Related Documentation

Documentation for Cisco Unified ICM/Unified Contact Center (IPCC) Enterprise & Hosted, as well as related documentation, is accessible from Cisco.com at **http://www.cisco.com/web/psa/products/index.html** (http://www.cisco.com/web/psa/products/index.html).

- Related documentation includes the documentation sets for Cisco CTI Object Server (CTI OS), Cisco Agent Desktop (CAD), Cisco Agent Desktop - Browser Edition (CAD-BE), Cisco Unified Contact Center Management Portal, Cisco Unified Customer Voice Portal (CVP), Cisco IP IVR, Cisco Support Tools, and Cisco Remote Monitoring Suite (RMS).

  For documentation for these Cisco Unified Contact Center Products, go to **http://www.cisco.com/web/psa/products/index.html** click on **Voice and Unified Communications**, then click on **Cisco Unified Contact Center Products** or **Cisco Unified Voice Self-Service Products**, then click on the product/option you are interested in.

- Also related is the documentation for Cisco Unified Communications Manager, which can also be accessed from **http://www.cisco.com/en/US/support/index.html** (http://www.cisco.com/web/psa/products/index.html)

- Technical Support documentation and tools can be accessed from **http://www.cisco.com/en/US/support/index.html**

- The Product Alert tool can be accessed through (login required) **http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice**

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit > Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention.

Convention	Description
	• A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco CRS Installation Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: **`<html><title>Cisco Systems,Inc. </title></html>`**
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Documentation Feedback

You can provide comments about this document by sending email to the following address:

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.

Documentation Feedback

Part 1: Pre-upgrade Preparation

Chapter 1

ICM/IPCC Upgrade Planning

Upgrade Planning

When planning to upgrade your ICM/IPCC 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

It is necessary to consider the additional software that interfaces with the Cisco ICM software when planning your ICM/IPCC upgrade.

Examples of the additional software include:

- IPCC including CallManager and IP IVR

- CTI desktop/client
- Unity
- Personal Assistant
- Auto Attendant
- Recording solutions

Hardware Requirements

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

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

First, review the ICM 7.5(1) hardware and software specifications. The minimum hardware requirements to upgrade to ICM software Release 7.5(1) are found in the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

Perform System Integrity Tests

The purpose of testing is to validate basic Unified SCCE functionality and fault tolerance prior to, during, and after each step of the migration and upgrade process.

Perform test cases when side A is upgraded and running in non-fault tolerant mode, prior to the upgrade of side B. Test cases should be executed prior to the upgrade to identify a baseline. Perform the test cases again when the system is fully upgraded and running in duplex mode.

Perform system integrity tests to:

- verify that there are no unexpected errors reported in the ICM process windows
- verify that calls are flowing through the system using Internet Script Editor or Script Editor
- verify that you can run Real Time and Historical reports
- verify that you can make configuration changes

Network Inventory

Technology Refresh upgrade migration planning and execution require you draw a comprehensive and accurate system diagram detailing the Cisco ICM/IPCC 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 CallRouter to the recovering side CallRouter

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

Data Backup Plan

While you might perform normally scheduled backups of your data, you must define a plan for backing up and restoring system critical data just prior to commencing an upgrade migration. Refer to the following table 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).

System Critical Data	Common Ground Upgrade	Technology Refresh Upgrade
Backup the Logger SQL database(s).	Yes	No **Note:** Technology Refresh with EDMT performs a backup of the original database and restores it on the new system. If anything happens during EDMT, the original database is untouched.

System Critical Data	Common Ground Upgrade	Technology Refresh Upgrade
Backup the Historical Data Server (HDS) SQL database(s).	Yes	No **Note:** Technology Refresh with EDMT performs a backup of the original database and restores it on the new system. If anything happens during EDMT, the original database is untouched.
Backup any custom databases.	Yes	Yes
Backup WVDB database on the Distributor AW.	Yes	Yes
Export the Cisco Systems, Inc. registry key on all production system nodes.	Yes	Yes
Copy the *icm* directory on all production system nodes.	Yes	Yes
WebView users must backup custom templates and the WVDB on the Distributor AW(s). The custom templates are in the \ICM\<instance>\AW\custom directory.	Yes	Yes

Pre-upgrade Preparation for All ICM Servers

Pre-upgrade preparation is an integral part of the upgrade process. Perform the following on all ICM servers to assist in recovery in the event of a catastrophic upgrade failure:

Step 1 Run the following commands and record output in the indicated files:

- Run: **`ipconfig -all`** Save results in *ipconfig.txt*.
- Command: **`route print -p`** Save results in *route.txt*.
- Command: **`netstat -a -n`** Save results in *netstat.txt*.

Step 2 Save the *hosts* file.

Step 3 Save the *LMhosts* file if applicable.

Network Configuration Backup

You must 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 ICM/IPCC production system to your new ICM/IPCC system, the production system is going to be down for a short period of time until the cross over is complete.

Test Plan

Execute test cases at various stages of the upgrade based on your expectations. You must, at a minimum, 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.

See Also

Upgrade Planning on page 11

Schedule of Activities

Due to the complexity of an ICM/IPCC production system, you must 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 ICM/IPCC nodes to be upgraded and their upgrade status.

Upgrades are usually performed during off-peak hours. Keep in mind that you might require more than one upgrade window. Normally, an initial maintenance window is established to get the ICM/IPCC 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 ICM/IPCC Release 7.5(1) before bringing them online.

Definition of Upgrade Steps

The upgrade migration of an ICM/IPCC 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 ICM/IPCC 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 the Test Plan section).

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)

See the Run Post-Upgrade tests section for additional details.

Stakeholder Notification

The following ICM/IPCC 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

Related Documents

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

Review and have available the following documents when performing an ICM/IPCC 7.0(x), 7.1(x), or 7.2(x) to ICM/IPCC 7.5(1) system upgrade:

- **Cisco ICM/IPCC Software Documentation Set** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/tsd_products_support_series_home.html)

  Note: Carefully scrutinize the documentation set to ensure you understand the impact of the upgrade process on any key functionality.

- *Release Notes for Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.5(1)*

Part 2: ICM/IPCC Software Upgrade

Chapter 2

Getting to the Baseline

Prior to commencing an upgrade to ICM/IPCC 7.5(1), ensure your system meets all of the applicable baseline requirements.

Baseline Requirements

The baseline requirements are as follows:

- All ICM nodes (CallRouter, Logger, NICs, AWs, PGs, CTI Server) at ICM/IPCC 7.0(x), 7.1(x), or 7.2(x).

  Note: The ICM/IPCC 7.0(x), 7.1(x), or 7.2(x) systems must be functioning prior to upgrade. Minimal functional requirements are: version and most recent Maintenance Release are installed on all components, the Logger data has completed entire migration process (which includes completion of data migration), Historical Data Server has completed replication (post upgrade), all components and features are functioning properly.

- All ICM/IPCC nodes running Windows 2000 Server SP4 or Windows Server 2003.

  Note: Prior to executing a Common Ground upgrade, the Active Directory Domain Controller and DNS functionality must be moved off of any ICM components. Refer to "Migrating Active Directory and DNS to a Non-ICM Server" for additional information.

- Logger, AWs, and HDS running SQL Server 2000 SP4 or SQL Server 2005 (for TR upgrades only).

- CAD at Release 6.0, 7.0, 7.1, or 7.2. See the Cisco CAD Installation Guide for specific operating system requirements.

- CTI OS desktops at Version 7.0(x), 7.1(x), or 7.2(x).

- CEM, CCS, CMB at Version 6.0, 7.0, or 7.5.

- DCA at Version 2.1.
- CCM at Version 4.1, 4.2, 5.0, or 6. 0 with the compatible IP IVR or CVP (ISN) version as per the Cisco IP Contact Center Enterprise Edition Software Compatibility Guide.

  Note: Refer to the Cisco IP Contact Center Enterprise Edition Software Compatibility Guide for the compatibility between the Cisco CallManager version and the IP IVR and/or CVP version.

- ACDs at a version compatible with ICM/IPCC 7.5(1).

  Note: Refer to the Cisco ICM Software Supported Switches (ACDs) document for ACD compatibility information.

- Hardware meets specifications in the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html). The hardware required for both Technology Refresh and Common Ground upgrades is specified.

  Note: If existing hardware is to be reused, verify that CPU and memory usage is below 50% utilization prior to the upgrade. If CPU or memory usage is above 50%, or if new feature usage or capacity increases (higher agent count, increased call rate, ECC increases) are planned, then new hardware should be deployed.

- Active Directory Environment must be created and configured for ICM/IPCC.

  Note: Refer to the Active Directory Considerations for Upgrades (page 51) for detailed upgrade information.

- Windows firewall configuration scripts must be run to enable network connectivity.
- ICM/IPCC Support Tools Server upgraded to Release 2.3(1).

  Note: Refer to the Support Tools Considerations for Upgrades (page 51) for detailed upgrade information.

- Perform backup of existing servers and verify backups

Chapter 3

Common Ground Upgrades vs. Technology Refresh Upgrades

ICM/IPCC Upgrade Methods

There are two supported ICM/IPCC upgrade methods:

- **Common Ground (CG)**

  The Common Ground upgrade method is performed in place on the existing hardware if the hardware has been evaluated and determined to meet the minimum requirements for Cisco ICM/IP Contact Center, Release 7.5(1).

- **Technology Refresh (TR)**

  The technology Refresh upgrade method is performed when you decide to (or it is required that) upgrade your hardware as well as your Cisco ICM/IPCC software and supporting third party software. The upgrade method consists of transporting all data, customized files/information, and related registry keys to the new hardware previously configured with a compatible operating system and database server (where required); then upgrading the transported data to a new release of Cisco software.

  Note: Upgrades involving Common Ground Upgrades on some ICM/IPCC nodes and Technology Refresh on others are supported, however, the A and B side of any given component must be running on identical hardware.

Chapter 4

Introduction to ICM/IPCC Upgrade

Upgrading a Cisco ICM/IPCC system involves numerous steps and the upgrade order of operation is distinct. From your initial software load, you may need to upgrade the operating system, the ICM/IPCC software (and options), the database software, and any required third party software.

Warning: In order to complete an upgrade successfully, the order of upgrade as defined in this guide MUST be followed.

ICM/IPCC Upgrade Overview

A full ICM/IPCC system is made up of several individual components or nodes which can be geographically dispersed. In moderate to large systems, it is not possible to upgrade all ICM/IPCC components in the same maintenance window. The ICM/IPCC upgrade process allows the full system to be upgraded over multiple maintenance windows.

This upgrade process applies to both Cisco ICM/IP Contact Center Enterprise and Hosted editions.

Note: Prior to upgrading a production system, you are encouraged to perform the upgrade on a lab system which mirrors your production system.

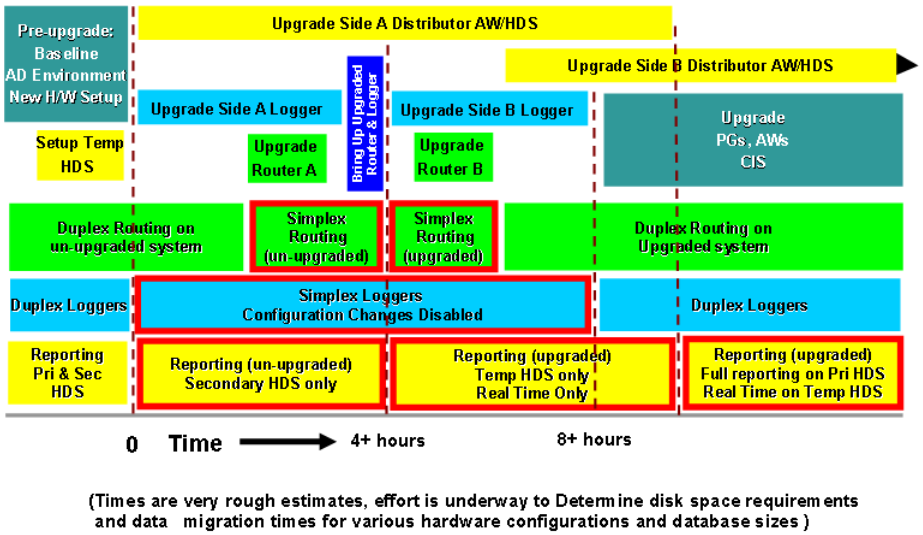
Refer to Upgrade Procedures (page 101). Select the example that is most applicable to your ICM/IPCC system. Refer to the Upgrade Checklists (page 177) section for the checklist associated with the previously chosen example procedure. Modify the checklist to suit your specific situation, then use the modified checklist as a guide and record of progress throughout the upgrade process.

High Level ICM/IPCC 7.5(1) Upgrade Overview

Before you upgrade to ICM/IPCC 7.5(1), make sure your systems are in compliance with the upgrade baseline requirements (page 21). If not, use the upgrade process as documented for previous releases to get the system to the required baseline.

The following upgrade process overview outlines the high level steps to upgrade a complex, multi-media, ICM/IPCC system.

Figure 1: Upgrading a Complex, Multi-media, ICM/IPCC System



High Level Upgrade Overview

1. Bring the system to the pre-upgrade baseline (page 21).
2. Perform a system backup.
3. Setup the new hardware and the Active Directory environment.
4. Upgrade the Side A Central Controller .

Warning: In order to complete an upgrade successfully, the order of upgrade as defined in this guide MUST be followed.

5. Verify Side A operation, then bring Side A into service.
6. Upgrade the Side B Central Controller(CallRouter (page 139), Logger (page 133), Distributor AW and HDS (page 115), WebView Server (page 131), NICs).

   The following steps can be performed in any order.

7. Upgrade the Client Administrator Workstations.
8. Upgrade the Peripheral Gateways and associated Outbound Option dialers (must be upgraded at the same time as the Campaign Manager), and the CTI OS Servers.

9. No upgrade is required for the CIS components (CEM, CCS, CMB, DCA).
10. Upgrade the CTI OS desktops.
11. Upgrade the CAD Server and Desktops (must be done together).
12. Install Infomaker (for custom reports) on a dedicated server.

Note:

- In Hosted ICM/IPCC environments, the NAMs and CICMs can be upgraded separately and in any order, provided that NAM/CICM compatibility is adhered to. ICM/IPCC 7.5(1) NAM works with 7.0(x), 7.1(x) and 7.2(x) CICMs. ICM/IPCC 7.5(1) CICM works with 7.0(x), 7.1(x), and 7.2(x) NAMs.
- In Hosted ICM/IPCC environments, the NAMs and CICMs can be upgraded separately and in any order, provided that NAM/CICM compatibility is adhered to. ICM/IPCC 7.0(0) NAM works with 5.0(0) and 7.0(0) CICMs. ICM/IPCC 5.0(0) NAM works with 4.6.2, 5.0(0), and 7.0(0) CICMs. ICM/IPCC 6.0(0) is not supported in a hosted environment.

Chapter 5

ICM/IPCC 7.5(1) Upgrade Time and Space Requirements

Introduction

Successful upgrade planning requires an understanding of the time and space requirements necessary to upgrade the various ICM/IPCC components. The Logger and HDS upgrades take longer to upgrade than other ICM/IPCC nodes due to the time it takes to upgrade the HDS and Logger databases.

For technology refresh upgrades, the network configuration between the source and target hardware also effects the overall upgrade times.

A number of factors affect the database migration times:

The most critical parameters are:

- the overall database size
- the database profile
- the type of upgrade (Common Ground vs. Technology Refresh)
- ICM/IPCC 7.0(x), 7.1(x), or 7.2(1) to ICM/IPCC 7.5(1) upgrade
- the hardware involved, especially the efficiency of the disk subsystem (see Appendix D)

Database Migration Performance

Prerequisites

EDMT requires additional disk space in which to copy and modify data and data structures during the migration process. This requires that additional disk space is available to the database to allow the database, database log file, temp db, and temp db log file to be able to grow.

Calculate Necessary File Size

The following sections provide instructions on determining the requirements for your migration.

How to calculate the required disk space for the migration

Step 1 Use the ICMDBA tool to gather database information.

Step 2 Right-click on the database and select **Properties**.

Note: The Database Used Size = Percent Used of the Data Size Value.

Step 3 Determine and document the amount of rows and the size of the copy/drop tables.

To accomplish this:

- Select the database.
- Select **Data > Space Used Summary**.

  Note: The default setting lists the largest tables.

Step 4 Calculate the required disk space for the migration.

If none of the copy/drop tables have more than 7,000,000 rows:

- Determine the **DUS** (Database Used Size).
- Determine the required disk space for the database migration where:

  Required Disk Space = 2*DUS

If at least one of the tables listed above has more than 7,000,000 rows, and you are not able to reduce the row count(s) to less than 7,000,000 then:

- Determine the following values:

  TTSA (Total Table Size from all copy/drop tables

DUS (Database Used Size)

maxTSL (Table Size of the largest copy/drop table)

- Determine the database file size where:

  Required Disk Space = [(2*DUS) - TTSA] + (2*maxTSL)

Example for determining the disk space needed to complete the migration:

- Database Used Space (DUS) = 71,680 MB
- Copy/drop table size (TTSA) = 56,128 MB
- Largest Copy/drop table size (maxTSL) = 36,496 MB
- **Required Disk Space** = ((2 * 71,680) – 56,128) + 2(36,496) = **160,224 MB**

Temp DB Size

Step 1 Ensure the Temp DB Log is able to expand to 3 GB.

Step 2 Ensure the Temp DB Data is able to expand to 50% of the DUS.

Upgrade Paths

There are two Logger and HDS migration paths:

- Technology Refresh

  The Technology Refresh path is followed by customers replacing their existing Logger and/or HDS servers with new hardware.

- Common Ground

  The Common Ground path supports customers using the same Logger and/or HDS hardware to run ICM/IPCC 7.5(1).

The data migration set is identical regardless of the migration path one chooses to follow.

Technology Refresh involves:

- Backup/Copy/Restore
- Data Migration

Common Ground only involves:

- Data Migration

Time Guidelines and Migration Performance Values

Your best estimate of time and space requirements are generated by running EDMT against a copy of your production database, on hardware (see Appendix D) similar to your production environment, in a lab environment. For customers that do not have that ability the following subsections provide information gathered while performance testing in the labs (see Appendix E) at Cisco Systems, Inc.

Typical Database Migration Performance Values

The following table provides high level guidelines for the upgrade times for Loggers and HDSs based on the hardware (as defined in the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html) and the results observed during internal upgrade testing (see Appendix E). Actual times vary based on the parameters previously discussed.

Backup, Network Copy, and Restore – Technology Refresh Only

Copy speed is dependent upon the speed of the network and the speed of the disk sub-system. The faster the network the faster the copy completes.

Database Used Size (GB)	Backup/Copy/Restore Time (Hours)
10	.5 – 1
20	1.5 – 2.5
40	2 - 4
70	3.5 – 5

Note:

- The values in the **Database Used Size** in the table above are based on the amount of disk space used by the Source database, not the size of the disk it resides on.
- The **Backup/Copy/Restore Times** in the table above assume the network meets the minimum requirements of the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).
- For Technology Refresh upgrades, have the fastest network possible (gigabit through one network switch) between the source and the destination machines. Use of a crossover cable is not recommended because it lacks buffer memory and can cause data loss.

Run Timings, Technology Refresh and Common Ground

The conversion should take place in less than a half hour—in most cases, much less. Actual times will vary based on the parameters discussed in the Introduction to ICM/IPCC Upgrade (page 25).

Performance Considerations

During internal testing, hyper-threading has consistently doubled the time it took the database migration to complete; therefore, to minimize migration time one should disable hyper-threading.

Ways to Reduce Data Migration Time

How to reduce data migration time:

- Reduce database size.
  - Purge the Logger DB of all data already replicated to the HDS (25 GB or less)
  - Remove any unneeded records, especially RCD, RCV, TCD, and TCV tables via ICM Purge Utility and/or SQL Query Analyzer.

    Note: Removing records impacts the availability of historical reports. Knowledge of the HDS schema is required.
- Use better hardware, especially on I/O subsystems.
  - RAID 1 + 0
  - I/O Cache – more is better
- For Technology Refresh upgrades, have the fastest network possible (gigabit through one network switch) between the source and the destination machines. Use of a crossover cable is not recommended because it lacks buffer memory and can cause data loss.

Chapter 6

Setting Up the Hardware

Technology Refresh Hardware Upgrade Prerequisites

Before undertaking a Technology Refresh upgrade, it's important that the newly deployed servers be installed.

The Active Directory environment (whether corporate or dedicated to the ICM/IPCC applications) must be configured/staged. The Windows Firewall configuration scripts must be deployed before ICM/IPCC servers can accept network connections.

Note: Refer to the guidelines outlined in the **Staging Guide, ICM/IPCC Enterprise/Hosted, ICM/IPCC Software Release 7.x(y)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_installation_guides_list.html).

Prior to performing a Technology Refresh upgrade on an ICM/IPCC node, new Cisco ICM/IPCC 7.5(1) Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials) compliant hardware must have the following software installed:

- Windows 2003 including latest supported service pack
- SQL Server 2005 including latest supported Maintenance Release and required patches for the ICM/IPCC nodes which require SQL (Logger, HDS, Distributor AW)
- Release 2.3(1) Support Tools agent
- VNC, PC Anywhere, Virus scanning, and any other required/desired third party software

Note:

- For additional information concerning the hardware and software requirements, refer to the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software**

Specification (Bill of Materials) (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)

- Cisco Security Agent must not be installed on the new servers until the appropriate step in the upgrade process. ICM setup checks for older versions of Cisco Security Agent and provides warnings or prevents continuation if an older version of CSA is installed or running.

Common Ground Hardware Upgrade Prerequisites

Before beginning a Common Ground upgrade, be sure that the existing hardware meets the requirements for ICM/IPCC 7.5(1) as specified in the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

Monitor CPU and memory usage to verify that there is sufficient “head room” to support the new release. If CPU or memory usage on the existing system is greater than 50%, it is necessary to upgrade the hardware.

How to set up the hardware

To accomplish this upgrade you must first:

- Stage all ICM/IPCC 7.5(1) machines in racks, or on a work surface, with the following:
  - RAM installed
  - Hard Drives installed
  - RAID arrays configured
  - Video and Ethernet Cards installed
  - All multiple rack mount systems occupying the same rack are attached to keyboard, mouse and monitor sharing unit
  - All machines are labeled with a hostname as per Network Design diagram.
  - All Ethernet connections are labeled “visible” or “private”.
  - There are sufficient power outlets for all machines to be simultaneously connected and turned on.
- Ensure there are at least 2 phone lines for testing of dial-up modem access
- Ensure all CDs (software), driver software on diskette or CD and Vendor documentation for all platforms are in the work area
- Ensure all Software License Numbers are available

- Ensure the simulated ICM Network is in place and successfully tested:
  - All LAN Switches are configured for required subnets per ICM System Diagram.
  - All IP CallRouters are configured as required
  - IP connectivity between all subnets has been successfully tested
  - Required Ethernet connections are in place between ICM platforms and LAN switches.
  - Required Packet prioritization has been configured on IP CallRouters

For addition Windows and SQL Server staging information, refer to the **Staging Guide, ICM/IPCC Enterprise/Hosted, ICM/IPCC Software Release 7.x(y)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_installation_guides_list.html)

Installing Microsoft Windows 2003

Note:

- For additional information on installing Microsoft Windows Server 2003, refer to the **Windows Server 2003 homepage** (http://www.microsoft.com/windowsserver2003/default.mspx)
- For additional information on the applicable Microsoft Windows Service Pack, refer to the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)

Upgrading from Windows 2000 to Windows Server 2003 - Common Ground Upgrades Only

Upgrading from Windows 2000 to Windows Server 2003 requires a considerable amount of planning and preparation. One of the first areas to consider is the source operating system revision and most importantly edition. It is important to determine the nearest equivalent target edition before engaging in the upgrade.

Note: It is only possible to upgrade to an equivalent or higher operating system. It is not possible to “downgrade” to a less powerful operating system, as some functionality might be lost in the process.

For example, it is not possible to upgrade a server OS from Windows 2000 Server (or other server products in the Windows 2000 family) to the Windows Server 2003, Web Edition without removing the earlier operating system and performing a new installation.

The following table outlines the relationships between the Windows Server 2000 and Windows Server 2003 editions.

Note: The Windows 2003 Web Edition is not supported for any ICM 7.5(1) node.

Table 1: Windows 2000 and Windows 2003 Relationships

Windows 2000 Server Family	Windows 2003 Family
Windows 2000 Server	Standard Edition
Windows 2000 Advanced Server	Enterprise Edition
No Equivalent	Web Edition

Before upgrading to Windows Server 2003, the computer being upgraded must meet the system requirements, and all hardware components and Third Party Software are compatible with the operating system. The hardware requirements for the Windows 2003 operating system are exceeded by the ICM hardware requirements specified in the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

Windows 2003 Hardware Compatibility

One of the most important steps to take before running Setup on a server is to confirm that the hardware is compatible with products in the Windows Server 2003 family. This is accomplished by running a pre-installation compatibility check from the OS Setup CD or by checking the hardware compatibility information available on the Microsoft Windows Server 2003 Web site. Also, as part of confirming hardware compatibility, check to see that you have obtained updated hardware device drivers and an updated system BIOS.

If a mass storage controller (such as a SCSI, RAID, or Fibre Channel adapter) is used for the server hard disk(s), confirm that it is compatible with products in the Windows Server 2003 family. If the controller is compatible with products in the Windows Server 2003 family, but the manufacturer has supplied a separate driver file for use with your operating system, obtain the file (on a floppy disk) before running the Windows 2003 setup. During the early part of Setup, a line at the bottom of the screen prompts you to press **F6**. Further prompts guides you in supplying the driver file to Setup so that it can gain access to the mass storage controller.

If you are not sure whether you must obtain a separate driver file from the manufacturer of your mass storage controller, you can try running Setup. If the controller is not supported by the driver files on the Setup CD, and therefore requires a driver file supplied by the hardware manufacturer, Setup stops and displays a message saying that no disk devices can be found, or displays an incomplete list of controllers. After you obtain the necessary driver file, restart Setup, and press **F6** when prompted.

Regardless of whether you run a pre-installation compatibility check, Setup checks hardware and software compatibility at the beginning of an upgrade or new installation and displays a report if there are incompatibilities.

For a comprehensive list of hardware and software supported by the Windows Server 2003 operating system, see the **Windows Server Catalog** (http://www.microsoft.com/windows/catalog/server/).

For more information, see **Windows Server 2003 Support** (http://www.microsoft.com/windowsserver2003/support/) or the online **Product Documentation for Windows Server 2003** (http://www.microsoft.com/windowsserver2003/proddoc/).

Active Directory Considerations for Common Ground Upgrades

In Windows Server 2003, Active Director domains can operate at three functional levels:

- Windows 2000 mixed (includes domain controllers running Windows 2000, Windows NT 4.0, and Windows Server 2003). This is the default setting.
- Windows 2000 native (includes domain controllers running Windows 2000 and Windows Server 2003)
- Windows Server 2003 (only includes domain controllers running Windows Server 2003)

Once all domain controllers are running on Windows Server 2003, you can raise the Domain and Forest Functionality to Windows Server 2003 by opening Active Directory Domains and Trusts, right-clicking the domain for which you want to raise functionality, and then clicking Raise Domain Functional Level.

Note: Once you raise the domain functional level, domain controllers running earlier operating systems cannot be introduced into the domain. For example, if you raise the domain functional level to Windows Server 2003, domain controllers running Windows 2000 Server cannot be added to that domain.

It's important to ensure that prior to the upgrade of ICM to Release 7.5(1), the Active Directory mode in Windows 2000 be set to native mode. This is required by the ICM application, which fails to create the necessary user accounts and groups in the domain if it isn't at least in this mode. ICM Setup, through the Domain Manager tool, has the ability to detect the domain mode and prevents users from installing the application if it finds that the Active Directory functional level (Windows Server 2003) or mode (Windows 2000) is running mixed.

References: **How to upgrade Windows 2000 domain controllers to Windows Server 2003** (http://support.microsoft.com/default.aspx?scid=kb;en-us;325379)

This article discusses how to upgrade Microsoft Windows 2000 domain controllers to Microsoft Windows Server 2003 and how to add new Windows Server 2003 domain controllers to Windows 2000 domains.

Internet Information Services (IIS) 6.0 Considerations for Common Ground Upgrades

When upgrading from Windows 2000 Server with IIS 5.0 to one of the following operating systems:

- Windows Server 2003 operating system, Standard Edition
- Windows Server 2003 operating system, Enterprise Edition

The World Wide Web Publishing Service (WWW service) is not enabled by default due to increased security measures. If you have already upgraded, you can start the WWW service by using the Services snap-in.

If you have not yet upgraded and you want the WWW service to be enabled by default after you upgrade, you must perform one of the following steps before you start the upgrade:

- If you have not already done so, run the IIS Lockdown Tool on the computer that you want to upgrade. The IIS Lockdown Tool reduces the web server's exposure to attack by disabling unnecessary features and giving you the choice to enable and customize features for your site. This tool is available from the Microsoft Web site. A description of how to run this tool is detailed in the Security Best Practices Guide for Cisco ICM 7.5(1).
- Create the registry key RetainW3SVCStatus under the node: yahoo

  \SYSTEM\CurrentControlSet\Services\W3SVC, and then add a DWORD value of any name equal to 1.

  For example, create the key:
  KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC
  \RetainW3SVCStatus\do_not_disable with the DWORD value of 1.
- Add the entry "DisableWebServiceOnUpgrade = false" to the script that you use to perform an unattended installation. After the upgrade is complete, ensure that all unnecessary IIS features have been removed or disabled and that the enabled features are configured with the highest security settings that your organization can support.

Operating System Upgrade Considerations for WebView

When upgrading the Operating System on a server with WebView Server installed, the following steps must be performed:

Step 1 Upgrade the operating system to Windows 2003 with the latest supported service pack.

Note: For additional information on the applicable Microsoft Windows Service Pack, refer to the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

Step 2 Run the ICM Third-Party Installer and re-install the New Atlanta ServletExec ISAPI component.

Note: The JDK or EA Server must not be re-installed.

Step 3 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD on the WebView server. Edit the WebView component and continue all the way through setup for the component to re-install and re-configure the WebView files.

Installing Microsoft SQL Server 2005

SQL Server 2005 is supported with the 7.5(1) release.

Note: When performing a Technology Refresh upgrade on an AW, SQL Server must be installed on the same drive on the new server. For example: If SQL Server was installed on the C: drive of the source server, it must be on the C: drive of the destination server.

The following is an overview of the SQL Server 2005 installation:

1. Copy all of the files on the SQL Server 2005 CD to a directory on your drive.
2. Install SQL Server 2005.
3. Run the SQL Server Configuration Manager to configure the Client Protocols.
4. Install the SQL Server service pack(s).

How to Install Microsoft SQL Server 2005

In ICM/IPCC 7.5(1), SQL Server 2005 is only installed on Loggers, HDS, or AWs.

Note: In System IPCC 7.5(1), these core components are referred to as the Central Controller and Administration and WebView Reporting machine.

Step 1 Run **autorun.exe**.

Step 2 On the Start screen, select **Server components, tools, Books Online, and samples** to start SQL Server setup.

The Software License Agreement screen appears.

Step 3 Read the terms of the license agreement.

a. Check **I accept the licensing terms and conditions**.

b. Click **Next**.

The Installing Prerequisites screen appears.

Step 4 Click **Install**.

The Welcome to the Microsoft SQL Server Installation Wizard screen appears.

Step 5 Click **Next**.

The System Configuration Check screen appears.

Step 6 When the system configuration check completes successfully, click **Next**.

The Microsoft SQL Server Installation screen appears.

Step 7 When the installation has completed, click **Next**.

The Registration Information screen appears.

Step 8 Complete the Name, Company, and Product Key fields, then click **Next**.

The Components to Install screen appears.

Step 9 Select **SQL Server Database Services** and **Workstation components, Books Online and development tools**, then click **Next**.

The Instance Name screen appears.

Step 10 Select **Default instance**, then click **Next**.

The Service Account screen appears.

Step 11 Select **Use a domain user_account**, then complete the Username, Password, and Domain fields.

Step 12 In the Start services at the end of setup section select **SQL Server** and **SQL Server Agent**, then click **Next**.

The Authentication Mode screen appears.

Step 13 Select **Windows Authentication Mode** or **Mixed Mode (Windows Authentication and SQL Server Authentication)** as appropriate.

If **Mixed Mode (Windows Authentication and SQL Server Authentication)** is selected, you must provide the sa logon password and confirm it.

Note: The sa user must have read access to the ICM Logger database.

Step 14 Click **Next**.

The Collation Settings screen appears.

Step 15 Select **Collation designer and sort order**, then select **Latin 1_General** from the drop-down list.

Step 16 Select **Binary**, then click **Next**.

The Error and Usage Report Settings screen appears. You have the option of selecting either error and reporting selection, or neither.

Step 17 After making your choice, click **Next**.

The Ready to Install screen appears.

Step 18 After reviewing the components to be installed, click **Install**.

The Setup Progress screen appears and the installation begins.

Step 19 When the installation has completed, click **Next**.

The Completing Microsoft SQL Server 2005 Setup screen appears.

Step 20 After reviewing the provided information, click **Finish**.

The SQL Server 2005 installation is complete.

Step 21 Select **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager**.

The SQL Server Configuration Manager appears.

Step 22 Expand **SQL Native Client Configuration** and select **Client Protocols**.

A list of the client protocols appears to the right.

The correct order and states are:

1. **Shared Memory** - Enabled
2. **Named Pipes** - Enabled
3. **TCP/IP** - Enabled
4. **VIA** - Disabled

Step 23 If the order/state is not as indicated in the previous step, right-click **Client Protocols** and select **Properties**.

The Client Protocol Properties dialog appears. Use the dialog controls to ensure that the client protocols are in the correct position.

Step 24 Click **OK**.

The Client Protocol Properties dialog closes.

Step 25 Expand the SQL Server Network Configuration and select **Protocols for MS SQL Server**.

Step 26 Ensure that **Named Pipes** and **TCP/IP** are in the Enabled Protocols section. If either is not, right-click the disabled protocol name and select **Enable**. Ensure **VIA** is in the Disabled Protocols section.

Step 27 On the Menu bar select **File > Exit**.

The SQL Server Configuration Manager closes.

Step 28 Install the appropriate SQL Server Service Pack.

Note:

- In "Services", the Distributed Transaction Coordinator must be set to **Automatic** and running prior to applying the service Pack.
- For additional information on the applicable Microsoft SQL Server Service Pack, refer to the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

a. Download the appropriate SQL Server service pack from the Microsoft web site.

b. Following the instructions provided with the service pack, install it.

Upgrading from SQL Server 2000 to SQL Server 2005 - Common Ground Upgrades Only

Upgrading from SQL Server 2000 to SQL Server 2005 is only done during an in-place Common Ground upgrade. Recognizing the significant impact of a SQL Server deployment in the upgrade scenario, Cisco continues to provide SQL Server 2000 support, provided that customers subsequently migrate to SQL Server 2005 within 90 days of the upgrade.

Note: Ensure the Distributed Transaction Coordinator service is running on the system during the upgrade to SQL Server 2005 or the COM+ Catalog Requirement outputs a warning message due to our security hardening. Start the Distributed Transaction Coordinator service in the Services MMC > Distributed Transaction Coordinator.

You must run Setup as an administrator. If you install SQL Server from a remote share, you must use a domain account that has read and execute permissions on the remote share.

Note:

- MDAC 2.8 must be installed prior to upgrading from SQL Server 2000 to SQL Server 2005 or the component installation and microsoft.sqlserver.notificationservices.dll in the COM+ catalog fail to install.
- Ensure the MS Distributed Transaction Coordinator service is not disabled (set to Automatic or Manual) prior to upgrading SQL Server 2000 to SQL Server 2005. Failure to do so results in a COM Plus Catalog warning message in the System Configuration Check dialog and the upgrade fails.
- If you upgrade SQL Server 2000 to SQL Server 2005, ensure that you modify the registry key (**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.1\Setup = Resume**) value from 1 to 0. Then, install SQL Service pack 2. If you do not modify the registry key value, your database will fail to upgrade.

How to Upgrade SQL Server 2000 to SQL Server 2005

To perform an in-place upgrade, perform the following steps:

Step 1 Start the SQL Server 2005 Setup program and install the prerequisite software. Insert the SQL Server 2005 product CD or DVD into your computer CD or DVD drive. The SQL Server Installation Wizard starts automatically.

Note:

- If the SQL Server Installation Wizard does not start automatically, double-click **Splash.hta** in the root folder of the CD or DVD.
- To run Setup from a network drive, navigate to the installation location on the shared drive, and then double-click **Splash.hta**.

Step 2 To begin the installation process, click **Install SQL Server**.

The End User License Agreement dialog appears.

Step 3 Read the license agreement on the End User License Agreement dialog, click the checkbox to accept the licensing terms and conditions, then click **Next**.

The SQL Server Component dialog appears. SQL Server Express is installed by running SQLEXPR.EXE. The prerequisite Microsoft SQL Native Client and Microsoft SQL Server 2005 Setup Support files are installed, and the setup program copies and installs all supporting files on the target system.

Step 4 On the SQL Server Component Update dialog, Setup installs software required for SQL Server 2005. To begin the component update process, click **Install**. After the update completes, click **Finish**.

The Welcome dialog appears.

Step 5 On the Welcome dialog of the SQL Server Installation Wizard, click **Next** to continue.

The System Configuration Check dialog appears and the installation computer is scanned for conditions that may block Setup.

Step 6 Perform the system configuration checks.

The Setup program runs the system configuration checks before the actual setup begins to verify that the system meets the minimum criteria for installation and detects any pending reboot requirements.

To display a list of check items grouped by result, click **Filter** and then select a category from the drop-down list.

To view a report of SCC results, click **Report** and then select an option from the drop-down list. Options include viewing the report, saving the report to a file, copying the report to the Clipboard, and sending the report as e-mail.

If your system fails the configuration tests, click the failed link for more information, then take the corrective action required.

Step 7 To proceed with Setup after the SCC scan completes, click **Continue**.

The Registration Information dialog appears.

Step 8 Provide Registration Information (Name and Company, for this release the product key is entered automatically) as necessary, then click **Next**.

The Components to Install dialog appears.

Step 9 Select the components for your installation. Click **Next** to continue.

Note: By default, several features are turned off so you must explicitly choose the components you want to install. Be sure to select the **SQL Server Database Services** component as well as the client toolsâ€"Workstation Components, Books Online and development tools. A description for each component group appears in the Components to be Installed pane when you select it. You can select any combination of check boxes.

Step 10 Click **OK**.

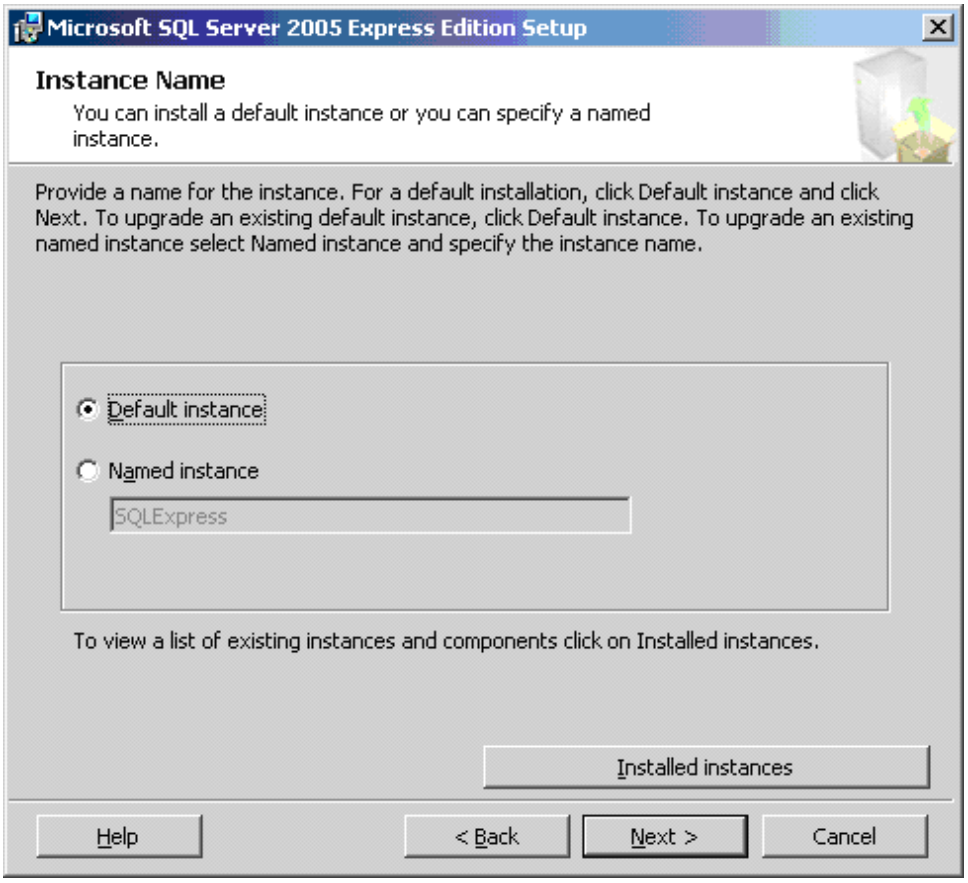
The Instance Name dialog appears.

Step 11 On the Instance Name dialog, select the **Default Instance** or a **Named instance** to upgrade.

The Setup program detects all installed instances using the MSI installation method and, by default, selects the default instance.

If a default or named instance is already installed, and you select an existing instance for your installation, Setup upgrades it and provides the option to install additional components.

Figure 2: Instance Name Dialog



a. To upgrade a SQL Server named instance already installed on your computer, click **Named Instance**, then type the instance name in the space provided; or click **Installed Instances**, select an instance from the Installed Instances list.

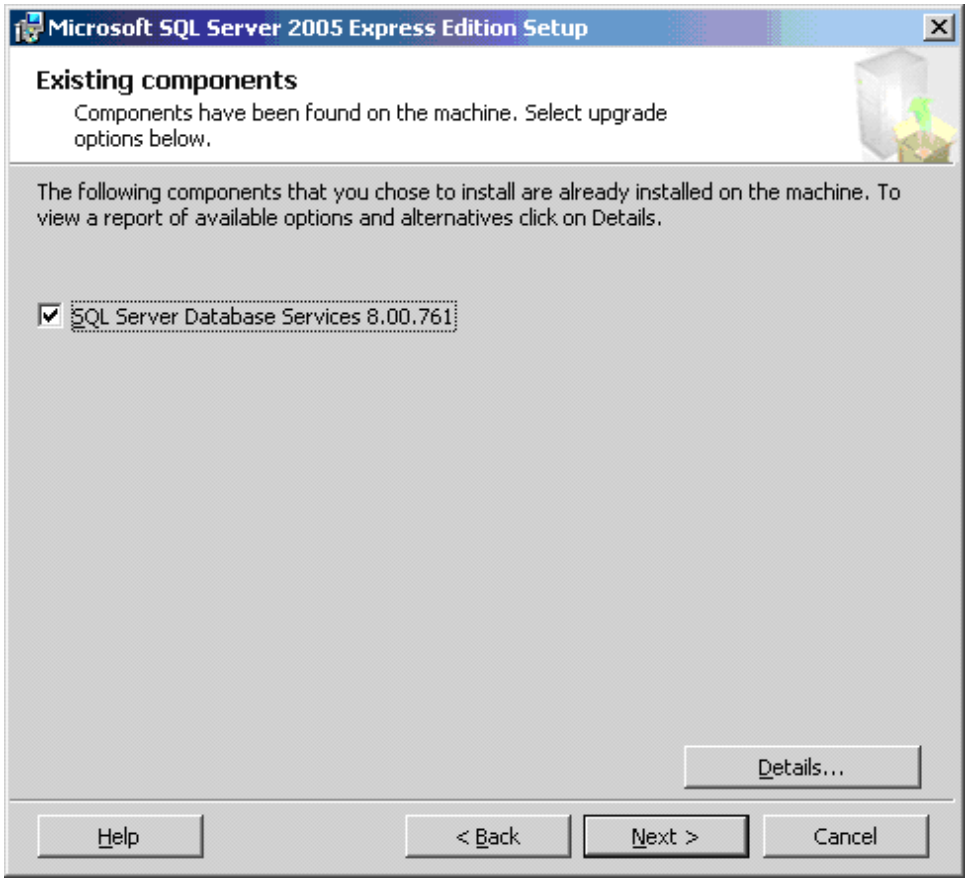
Note: To upgrade a default instance, there must be a default instance already on the computer. To upgrade a named instance, there must be a named instance already on the computer.

b. Click **OK** to populate the instance name field.

c. After you have selected the instance to upgrade, click **Next** to continue.

The Existing Components dialog appears.

Figure 3: Existing Components Dialog



Setup lists the SQL Server components installed on your computer. Components that can be upgraded to SQL Server 2005 have their check boxes enabled. If a component has a check box that is unavailable, the component does not qualify for upgrade to SQL Server 2005.

To view a report of available options and alternatives, click **Details**.

To upgrade a component listed on the Existing Components page, select its check box.

Step 12 Check **SQL Server Database Services 8.00.761**, then click **Next**.

The Service Account dialog appears.

Step 13 If necessary, add any required new components.

If you are adding new components, specify the user name, password, and domain name for the non-SQL Server accounts. For this release, SQL Server 2005 Setup uses the service account information of the existing SQL Server service being upgraded. You can use the same account for all of the services.

To optionally specify an individual account for each service, select **Customize for each service account**, select a service name from the list box, and then provide login credentials for each of the services in the list.

Note: The domain name cannot be a full Domain Name Service (DNS) name. For example, if your DNS name is my-domain-name.com, enter "my-domain-name" in the Domain text box. SQL Server Setup does not accept "my-domain-name.com" in the Domain text box.

Note: The Upgrade Logon Information page is displayed if the SQL Server instance to be upgraded is configured to use Mixed Mode (Windows Authentication or SQL Server Authentication). Credentials supplied on this page are used to connect to the existing SQL Server instance so that upgrade scripts can be run. If the existing SQL Server instance is configured to use Windows Authentication, this page is not displayed.

Step 14 Specify the logon information for the Setup program to use to connect to the instance being upgraded. Select the default option of **Windows Authentication**.

Click **Next**.

Note: For this release, SQL Server Setup may not enforce the strong password requirement on some default configurations of Microsoft Windows Server 2003 where the computer is not a member of a domain. Setting strong passwords is essential to the security of your system. Always use strong passwords.

Step 15 Specify the remaining configuration options (generally accept all defaults), and then click **Next**.

The Ready to Install dialog appears.

Step 16 Review the summary of features and components for your SQL Server upgrade scenario. All components and features of the existing instance are selected for the upgrade. To proceed, click **Install**.

The Installation Progress dialog appears.

Step 17 Monitor the upgrade progress as Setup proceeds.

Note:

- To view the log file for a component during the upgrade, click the product or status name on the Installation Progress dialog.
- On the Completing the Microsoft SQL Server Installation Wizard dialog, you can view the Setup summary log by clicking the link provided.

Step 18 Click **Finish** to exit the SQL Server Installation Wizard.

Step 19 If you are instructed to restart the computer, do so now.

Note: Failure to restart the computer may cause failures when you run the Setup program in the future.

Step 20 After restarting the computer, select **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager**.

The SQL Server Configuration Manager appears.

Step 21 Expand **SQL Native Client Configuration** and select **Client Protocols**.

A list of the client protocols appears to the right.

The correct order and states are:

1. **Shared Memory** - Enabled
2. **Named Pipes** - Enabled
3. **TCP/IP** - Enabled
4. **VIA** - Disabled

Step 22 If the order/state is not as indicated in the previous step, right-click **Client Protocols** and select **Properties**.

The Client Protocol Properties dialog appears. Use the dialog controls to ensure that the client protocols are in the correct position.

Step 23 Click **OK**.

The Client Protocol Properties dialog closes.

Step 24 Expand the SQL Server Network Configuration and select **Protocols for MS SQL Server**.

Step 25 Ensure that **Named Pipes** and **TCP/IP** are in the Enabled Protocols section. If either is not, right-click the disabled protocol name and select **Enable**. Ensure **VIA** is in the Disabled Protocols section.

Step 26 On the Menu bar select **File > Exit**.

The SQL Server Configuration Manager closes.

Step 27 Install the appropriate SQL Server Service Pack.

Note:

- In "Services", the Distributed Transaction Coordinator must be set to Automatic and running prior to applying the service Pack.
- For additional information on the applicable Microsoft SQL Server Service Pack, refer to the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System SoftwareSpecification (Bill of Materials)** ((http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)).

a. Download the appropriate SQL Server service pack from the Microsoft web site.

b. Following the instructions provided with the service pack, install it.

Support Tools Considerations for Upgrades

Before upgrading any of the ICM Core components (using either the Technology Refresh or the Common Ground method), upgrade the existing ICM Support Tools server to Release 2.3(1). This is required for compatibility with the Release 2.3(1) Support Tools agents which is installed on the ICM nodes during the upgrade process. The Release 2.3(1) Support Tools server is compatible with older Support Tools agents.

Active Directory and DNS Considerations for Upgrades

Active Directory Considerations for Technology Refresh Upgrades

The new servers must be in the Active Directory domain in the appropriate ICM organization unit. IP connectivity and remote access must be validated.

For the ICM/IPCC 7.5(1) release, the Logger cannot be the AD domain controller. When setting up the Active Directory environment, if the existing Loggers are also domain controllers, it may be necessary to migrate the domain controller roles to new non-ICM servers prior to the upgrade. Using the Active Directory tools provided with the Windows operating system, bring up the new domain controllers on the domain in which the ICM operates, transfer any applicable flexible single master operations (FSMO) roles, and then demote the domain controller on the production Logger to a member server. Refer to "Migrating Active Directory and DNS to a Non-ICM Server" for additional information.

Note: The Windows 2000 operating system is not supported for ICM/IPCC Release 7.5(1) Technology Refresh upgrades.

Active Directory Considerations for Common Ground Upgrades

Before undertaking a Common Ground upgrade, the Active Directory environment (whether corporate or dedicated to the ICM/IPCC applications) be configured or staged. The Windows Firewall configuration scripts must be deployed before ICM/IPCC servers can accept network connections.

For additional information, refer to the guidelines outlined in the **Staging Guide, ICM/IPCC Enterprise/Hosted, ICM/IPCC Software Release 7.x(y)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_installation_guides_list.html)

The new Active Directory environment must be set up prior to beginning the upgrade process. For the ICM/IPCC 7.5(1) release, the Loggers cannot host the AD domain controllers. If this is the existing configuration, it is necessary to migrate the domain controllers to a non-ICM servers. Perform the AD and DNS migration well in advance of the actual upgrade to allow time for implementation and stabilization. Repeat this for all Domain Controllers currently on ICM servers. Use the Active Directory tools provided with the Windows operating system, and bring up the new domain controllers on the domain in which the ICM operates. Transfer any

applicable flexible single master operations (FSMO) roles, and then demote the domain controllers on the Logger to member servers. Refer to "Migrating Active Directory and DNS to a Non-ICM Server" for additional information.

Note: This process may require the Logger to be down during demotion and transfer of the domain controller.

The operating system must be Windows 2003 (and the appropriate service pack) on all ICM core components or Windows XP on client AWs.

The Vista operating system is supported for ICM client AWs and Internet Script Editor. For System IPCC, Vista is also supported for the CTI OS desktop clients.

There are two methods by which you can ensure your systems are hardened:

1. Before engaging in the upgrade of the application, apply the security best practices outlined in the Security Best Practices Guide for Release 7.5(1).

2. After upgrading the application on Windows 2000, upgrade the Operating System to Windows Server 2003 and apply the automated hardening provided by the application at this OS revision. This can be accomplished by re-running ICM setup and choosing to apply the hardening when prompted, or by apply the security hardening from the command line as outlined in the Release 7.5(1) Security Best Practices Guide for Windows Server 2003.

Migrating Active Directory and DNS to Non-ICM Servers

Perform the AD and DNS migration well in advance of the actual upgrade to allow time for implementation and stabilization. Repeat this for all Domain Controllers currently on ICM servers.

Overview

- Using the Active Directory tools provided with the Windows operating system, bring up the new domain controllers on the domain in which the ICM operates.

  For additional information, refer to:

  – *How to install Active Directory on the new Domain Controller,*

  – *How to install DNS,*

  – *How to configure Active Directory sites on the new Domain Controller.*

- Transfer any applicable flexible single master operations (FSMO) roles and redefine the time source.

  For additional information, refer to:

  – your *ICM System Diagram* and the *ICM/IPCC System Design Specification* for your implementation.

  - *How to redefine the time source.*

- Set the new Domain Controller as the Global Catalog (if required).

  For additional information, refer to:

  - your *ICM System Diagram* and the *ICM/IPCC System Design Specification* for your implementation.

- Point all member servers to the new DNS servers.

  For additional information, refer to:

  - *How to configure member servers to point to the new DNS servers.*

- Demote the domain controller on the production Loggers to member servers.

  For additional information, refer to:

  - *How to demote current Domain Controllers to member servers.*

- Uninstall DNS from the 7.0(x), 7.1(x), and 7.2(x) ICM servers.

How to install Active Directory on the new Domain Controller

Step 1 Select **Start** > **Run** then enter **`dcpromo`** and click **OK**.

Step 2 When the Active Directory Wizard opens, click **Next**.

Step 3 Under *Domain Controller Type* select **Additional Domain Controller for an Existing Domain**.

Step 4 On the Network Credentials screen, enter the domain admin username and password.

Step 5 The Additional Domain Controller screen should already be filled in properly with the FQDN (Fully Qualified Domain Name).

Step 6 Accept the database and log location defaults.

Step 7 Accept the shared System Volume defaults.

Step 8 Enter the same Restore Mode Admin password that was utilized on the Root Domain Controller.

Step 9 Check **Summary Settings**. Active Directory is not configured via NETLOGON.

Step 10 Reboot when the Active Directory installation is complete.

Step 11 Repeat theses steps for a new alternate Domain Controller if necessary.

How to install DNS

Step 1 Select **Settings** > **Control Panel** > **Add/Remove Programs**.

Step 2 Select **Add\Remove Windows Components** then check **Networking Services** > **Details**.

Step 3 Check **DNS**.

Step 4 Select **OK** then click **Next**.

Step 5 Browse to the Windows 2000 CD – DNS installs.

Step 6 Validate that all DNS Zones were replicated from the 1st DNS Server in the Active Directory Domain, to this DNS Server.

Step 7 Repeat this installation for the new Secondary DNS server (if required).

How to configure Active Directory sites on the new Domain Controller

Step 1 Move the new Domain Controller to correct site(s).

How to move FSMO roles as indicated in the ICM System Diagram and per settings in your ICM/IPCC System Design Specification

Step 1 On the Active Directory Domain Controller hosting the role to be moved, open **AD Users and Computers**, then connect to the Domain Controller to which the role needs to be moved.

Step 2 Right-click under the domain name and select **Operations Masters**.

Step 3 Under the required FSMO role tab, change the Operations Master to this designated DC.

How to redefine the time source

Since the PDC Emulator is moving to another Domain Controller, the time source must be redefined as either that server or an external time source.

Step 1 On the server currently running the Primary Domain Controller Emulator, run the following command: **`Net time /setnstp: <DNS name of time source>`**

Step 2 To synchronize a member server to the time source, run the following command: **`W32tm /s: <DNS name of external time source>`**

How to assign Global Catalogs per the GC and FSMO plan in the ICM System Diagram and per settings in your ICM/IPCC System Design Specification

Step 1 Open **AD Sites and Services**.

Step 2 Connect to the Domain Controller designated as the Global Catalog.

Step 3 Right-click **NTDS Settings**, click **Properties**, check **Global Catalog**, and click **OK**.

Step 4 Repeat this procedure on all ICM servers.

How to configure member servers to point to the new DNS servers

Step 1 In the Network Settings, open the Visible network connection

Step 2 Open **TCP/IP properties**.

Step 3 Enter the new primary and alternate DNS servers.

Step 4 Run **`ipconfig /flushdns`** from a command prompt.

Step 5 Verify name resolution by pinging the ICM servers by name.

Step 6 Ping the ICM domain by name.

How to demote current Domain Controllers to member servers and uninstall DNS

Note: Important: Prior to demoting domain controllers make certain that the replication process from the old domain controllers to the new domain controllers has completed. Check the directory service with the event viewer to monitor the status. In a large domain it could be 30 minutes or more for this process to complete.

Step 1 Select **Start > Run**, then enter **`dcpromo`**. When the Active Directory Wizard opens, click **Next**.

Step 2 A dialog box indicating that this server is already a Domain Controller appears. Click **Next** to demote it to a member server.

Step 3 You are warned and prompted as to whether or not this is the last server in the domain. Leave the box unchecked and click **Next**.

Dialogs then show the progress of the Domain Controller removal.

Step 4 Click **Next** to finish.

Step 5 Repeat this procedure for the alternate Domain Controller.

Step 6 Select **Start > Settings > Control Panel > Add/Remove Programs**.

Step 7 Select **Add/Remove Windows Components > Networking Services**.

Step 8 Click **Details**.

Step 9 Uncheck **DNS**, then click **OK**.

Step 10 Click **Next**.

Perform System Integrity Tests

The purpose of the sample test cases in this section is to validate basic ICM functionality and fault tolerance prior to, during and after each step of the Migration Project. Refer to Appendix B for additional System Integrity test information.

Perform the following System Integrity Tests in the order listed:

- System Integrity Test 1 – Zero ICM Process Errors
- System Integrity Test 2 - RTTEST
- System Integrity Test 3 - OPCTEST
- System Integrity Test 4 - Call Router Fault Tolerance
- System Integrity Test 5 - PG Fault Tolerance
- System Integrity Test 6 - AW Configuration and Scripting Tools
- System Integrity Test 7 - Webview
- System Integrity Test 8 - Internet Script Editor

Verifying System Conditions Using EDMT

Verifying System Conditions for a CG Upgrade

Run EDMT on the system prior to the actual upgrade, to verify the following conditions:

- Connections to the source and destination databases are available
- The collation value for the source and destination databases is:
  - Latin1_General_BIN (for western/European languages -English, French, Spanish, German, etc.)

  - Japanese_BIN (for Japanese)
  - Chinese_PRC_BIN (for Chinese)
  - Korean_Wansung_BIN (for Korean)
  - The source and destination databases use the same collation value.
- The operating system is Windows 2003
- SQL Server 2000 or 2005 is installed
- The schema for the source is correct:
  - 95 for Unified ICM/CCE Release 7.0(0)
  - 96 for Unified ICM/CCE Release 7.1(1)
  - 97 for Unified ICM/CCE Release 7.2(1)

Once these checks are made, an **Are You Sure** dialog box is presented. If you are running EDMT only to perform these checks, cancel at this point.

Verifying System Conditions for a TR Upgrade

Run EDMT on the new hardware prior to the actual upgrade, to verify the following conditions:

- Connections to the source and destination databases are available
- The collation value for the source and destination databases is:
  - Latin1_General_BIN (for western/European languages -English, French, Spanish, German, etc.)
  - Japanese_BIN (for Japanese)
  - Chinese_PRC_BIN (for Chinese)
  - Korean_Wansung_BIN (for Korean)
  - The source and destination databases use the same collation value.
- The operating system is Windows 2003
- SQL Server 2000 or 2005 is installed
- The schema for the source is correct:
  - 95 for Unified ICM/CCE Release 7.0(0)
  - 96 for Unified ICM/CCE Release 7.1(1)

– 97 for Unified ICM/CCE Release 7.2(1)

Once these checks are made, an **Are You Sure** dialog box is presented. When these checks are complete, select **Cancel**.

Note: If adequate disk space is not available, a temporary server must be configured to store the data moved from the non-upgraded system. The temporary server need not have SQL Server installed. Using a temporary database server results in increased data migration times because the data is moved across the network twice instead of once. The temporary database server location is entered in the Backup Connection panel of the wizard. The upgrade procedures and times indicated in the following sections assume that a temporary server is not required.

When EDMT backs up the database from the production Logger or HDS, it stores the data in one backup file, even if the data section of the database is broken up into separate data files (data0, data1, data2, etc.), and/or the log section is broken up into separate files (log0, log1, log2, etc.).

Each of the files could potentially be on separate logical or physical disk drives. EDMT only allows one restore location. This is the desired Unified ICM configuration since the disk configuration of the new hardware must exactly match the configuration of the original system, and that may not make sense with newer hardware.

Chapter 7

Enhanced Database Migration Tool (EDMT) for ICM/IPCC 7.5(1)

Introduction

The ICM/IPCC 7.0(x), 7.1(x) and 7.2(x) Logger and HDS database schemas are migrated to the ICM/IPCC 7.5(1) database schema using the Enhanced Database Migration Tool (EDMT) during the upgrade process.

The Cisco ICM/IPCC Enhanced Database Migration Tool (EDMT) is a wizard application used to migrate the ICM/IPCC database during the ICM/IPCC upgrade process. It can be installed on the destination server (see Installing EDMT for additional information). The time required to complete a data migration varies in a direct relationship to the database size (the larger the database size, the longer it takes to migrate) and the server hardware performance level.

The EDMT requires prerequisites be completed (see the EDMT Installation Prerequisites (page 59) for additional information) prior to running the application (see Running the EDMT (page 60) for additional information).

This product includes software developed by:

- CDS Networks, Inc.
- the JDOM Project (http://www.jdom.org/)

EDMT Installation Prerequisites

Prior to installing the Enhanced Database Migration Tool (EDMT), prerequisite tasks must be performed.

Step 1 Using the Microsoft SQL Backup and Resore utility, create a backup copy of the source ICM/IPCC 7.0(x), 7.1(x) or 7.2(x) MS SQL Server database, as applicable.

EDMT Installation

Step 1 Download the **Cisco ICM/IPCC Enhanced Database Migration Tool** (http://www.cisco.com/kobayashi/sw-center/telephony/icm/icm-planner.shtml) .

Step 2 Select where you want to run the EDMT wizard from (it can be installed on the destination server for TR upgrades, on the source server for CG upgrades, or from the download).

Step 3 Navigate to the download and run **edmt.exe** to start the wizard (see Running the EDMT (page 60)).

Note: You may also run edmt.bat. The only difference between the two is that when running edmt.bat, the console window remains open.

Running EDMT

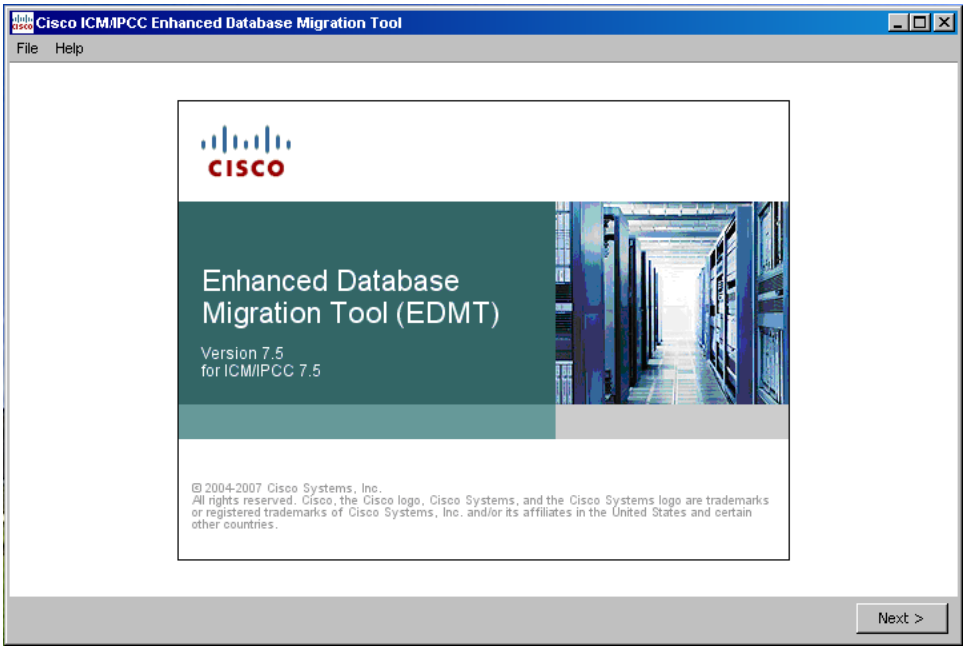
Once you have installed the Enhanced Database Migration Tool (EDMT), run the wizard to migrate the database. The following provides an overview of the steps to run the EDMT..

Note: Prior to running EDMT set the *Maximum file size* for the data files on the database to **Unrestricted growth**. Refer to How to set the tempdb database size (page 175) for additional information.

Step 1 Run **edmt.exe**, from the chosen location (see EDMT Installation (page 60)).

Regardless of the upgrade type, when you run edmt.exe, the first screen to appear is the splash screen.

Figure 4: EDMT Splash Screen



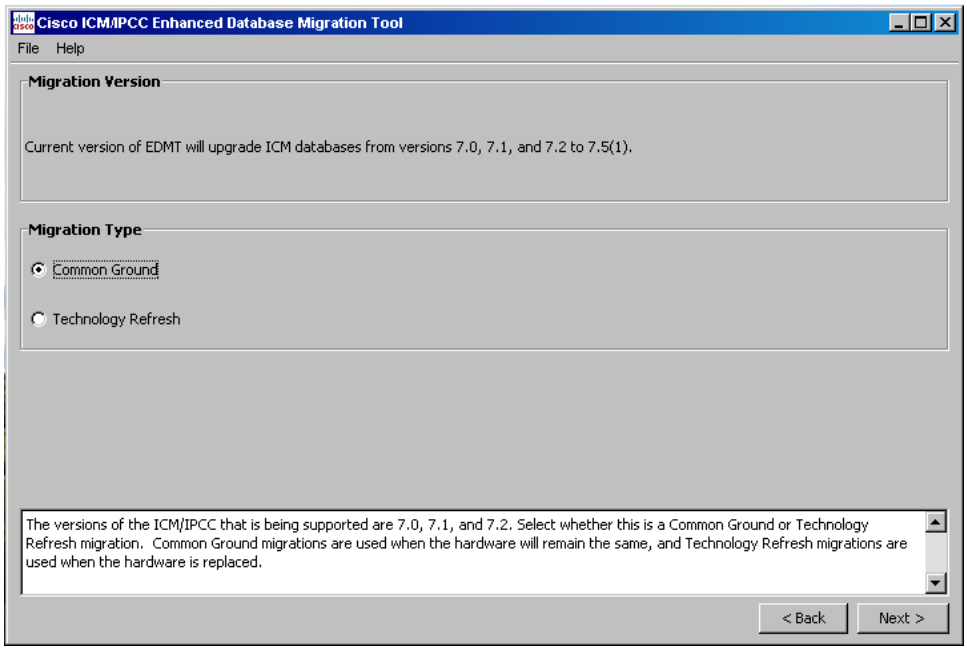
Once you select the Migration Type on the Migration Version/Migration Type screen and click **Next**, you begin a sequence of screens based on that selection.

Step 2 Click **Next**.

The Migration Version/Migration Type dialog appears.

The Migration Version/Migration Type dialog of the EDMT Wizard is common to both the Common Ground and the Technology Refresh upgrades. It contains two panels, the Migration Version panel and the Migration Type panel.

Figure 5: EDMT Migration Version/Migration Type Dialog



Refer to Migration Version/Type Dialog (page 71) for additional information on the Migration Version (page 71) and the Migration Type (page 71) properties.

Step 3 Select the appropriate migration type by clicking the appropriate radio button in the Migration Type panel.

A **Common Ground** migration means the Logger or HDS database is being migrated in place and the existing database schema modified from either ICM/IPCC 7.0(x), 7.1(x) or 7.2(x) to the level of ICM/IPCC 7.5(1). For this to occur, EDMT must be installed and run on the source database server being migrated. This migration is complete upon successful execution of the EDMT.

In the case of a **Technology Refresh** upgrade, EDMT must be installed and run on the new **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html) compliant destination database server machine. Once installed, running EDMT automatically performs a backup of the ICM/IPCC source database onto the new destination server. Next, EDMT restores the backup to the destination database and performs what amounts to a Common Ground migration on the newly restored ICM/IPCC 7.0(x), 7.1(x), or 7.2(x) database. The backup file created is automatically deleted. This migration is complete upon successful execution of the EDMT.

Step 4 Click **Next** to proceed with the selected migration type.

Note:

- The Migration Type selected here affects the sequence of the EDMT wizard panels displayed as you progress through the rest of the migration process. See EDMT Wizard Screen Sequences (page 63) for additional information.

- The EDMT shrinks the temp database back to the original size upon completion of the data migration.

EDMT Wizard Screen Sequences

Refer to the following migration type sequences for additional information:

- Common Ground EDMT Wizard Sequence (page 63)
- Technology Refresh EDMT Wizard Sequence (page 66)

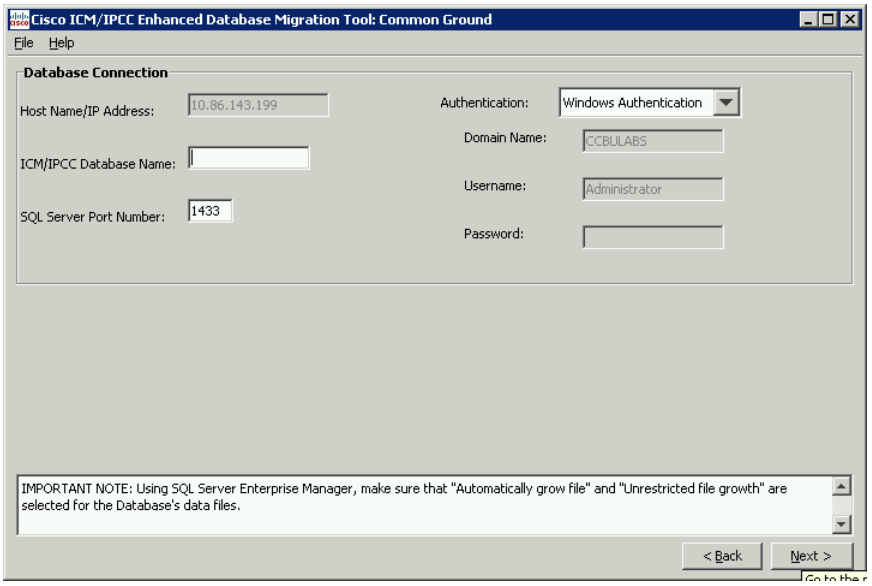
Common Ground EDMT Wizard Sequence

In the case of a Common Ground upgrade, EDMT must be installed and configured on the source database server machine.

After you select the **Common Ground** migration type and click **Next**, the following sequence of dialogs appears, starting with the Database Connection dialog.

Note: Once you click **Next** on the Migration Version/Type dialog, the title of the application changes to add the type of migration. Thus, the title becomes "Cisco ICM/IPCC Enhanced Database Migration Tool: Common Ground".

Figure 6: EDMT CG Database Connection Dialog



Refer to Database Connection Dialog (page 72) for additional information on the Database Connection properties.

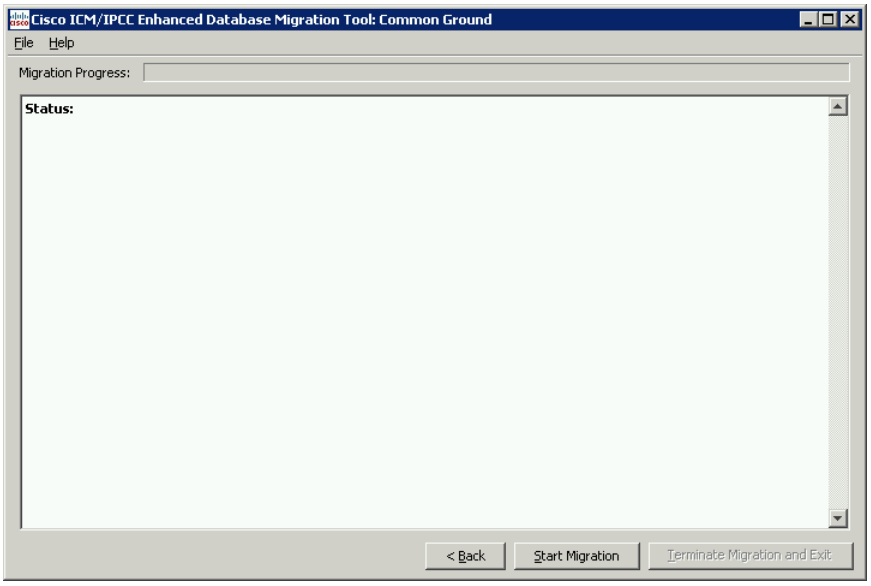
Step 1 On this panel, enter the information necessary to enable the EDMT to connect to the source database server during a Common Ground migration, then click **Next**.

Note: While you enter the required data on this panel, clicking **Next** does not make the actual connection. At this point the data entered is only checked for completeness prior to allowing you to continue. The connection does not take place until after you start the data migration by clicking **Start Migration** on the Migration Control dialog.

The Migration Control dialog appears.

This dialog allows you to start or terminate the data migration. It also displays the status of the data migration process.

Figure 7: EDMT CG Migration Progress Dialog - Before Starting Migration

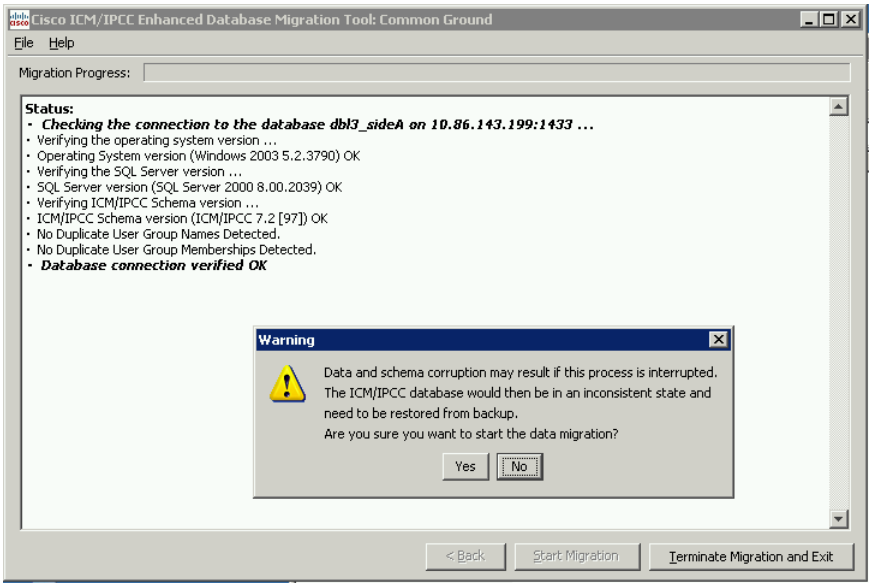


Refer to the Migration Control Dialog (page 74) for additional information on the Migration Control properties.

Step 2 Click **Start Migration** to begin the Common Ground database migration process.

The status of the migration process indicates that the database connection has been verified and a warning appears.

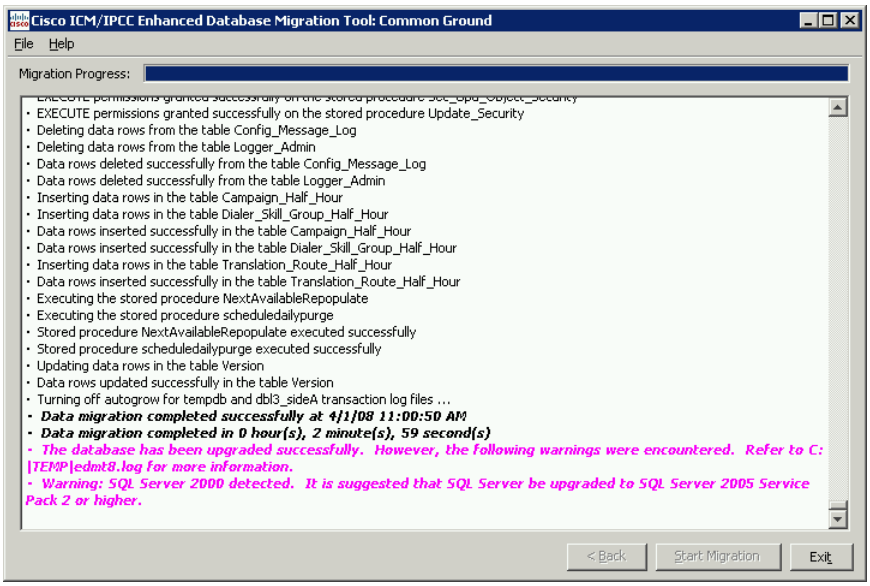
Figure 8: EDMT CG Migration Progress Dialog - After Starting Migration



Step 3 Click **Yes** and the Common Ground data migration begins.

The Migration Progress bar displays the progress of the migration while the Description field displays migration status messages.

Figure 9: EDMT CG Migration Progress Dialog - Migration Complete



Errors are displayed in bold, red, italic text.

Warnings are displayed in bold, magenta, italic text; and are repeated at the end of the migration as shown above.

Note: Warnings do not stop the migration process and the upgraded database is still usable. On the other hand, errors stop the migration process and leaves the database in a corrupt state. You

must restore the database from the backup you made prior to running EDMT if an error is encountered and you must run EDMT again after fixing whatever error is detected.

Step 4 Click **Exit** to close the EDMT.

Technology Refresh EDMT Wizard Sequence

In the case of a Technology Refresh upgrade, EDMT must be installed and configured on the new **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html) compliant destination database server machine. Once installed and configured, running EDMT automatically performs a backup of the ICM/IPCC source database onto the new destination server.

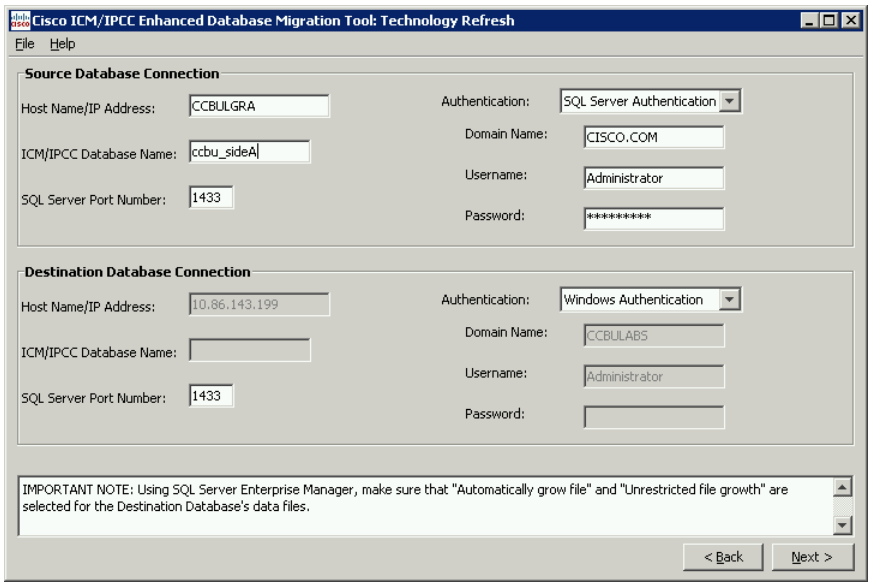
Note:

- Prior to running EDMT set the *Maximum file size* for the data files on the source database to **Unrestricted growth**. Refer to How to set the Logger or HDS database data file size for maximum growth (page 173) for additional information.
- If the reporting capabilities on a system with a single HDS must be maintained throughout the upgrade, it is necessary to create a temporary HDS database.

After you select the **Technology Refresh** migration type and click **Next**, the following sequence of dialogs appears, starting with the Database Connection dialog.

Note: Once you click **Next** on the Migration Version/Type dialog, the title of the application changes to add the type of migration. Thus, the title becomes "Cisco ICM/IPCC Enhanced Database Migration Tool: Technology Refresh".

Figure 10: EDMT TR Source/Destination Database Connection Dialog



This dialog requires you to enter the information necessary for the EDMT to connect to the migration source and migration destination database servers during a Technology Refresh migration.

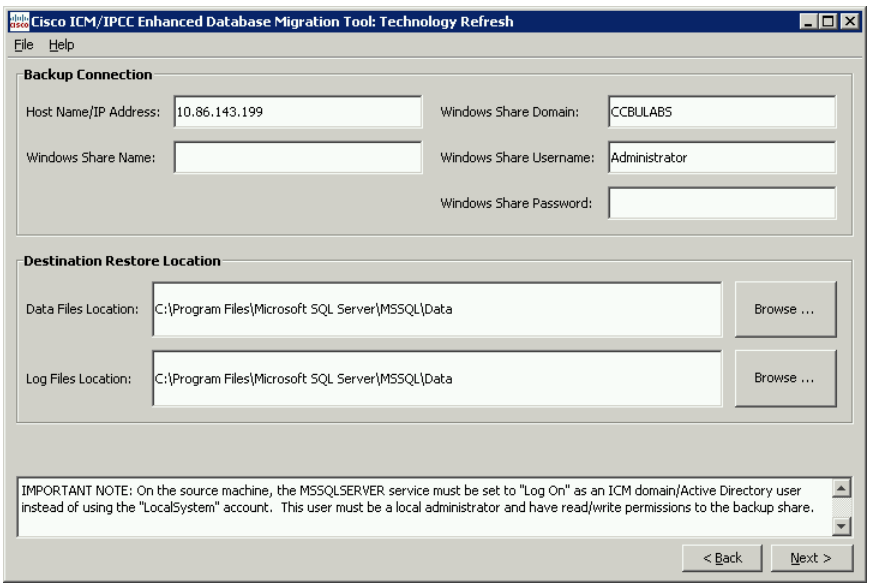
Refer to the Database Connection Dialog (page 72) for additional information on the Source Database Connection Panel Properties (page 72) and the Destination Database Connection Panel Properties (page 72).

Step 1 Provide the information required to allow the EDMT to connect to the source and destination databases, then click **Next**.

Note: While you enter the required data on this panel, clicking **Next** does not make the actual connection. At this point the data entered is only checked for completeness prior to allowing you to continue. The connection does not take place until after you start the data migration by clicking **Start Migration** on the Migration Control dialog.

The Backup/Restore dialog appears.

Figure 11: EDMT TR Backup Connection/Destination Restore Location Dialog



Refer to the Backup/Restore Dialog (page 73) for additional information on the Backup Connection Panel Properties (page 73) and the Destination Restore Location Panel Properties (page 74).

The Backup Connection panel requires you to enter the information necessary for EDMT to backup the migration source database during a Technology Refresh migration.

The Restore Location panel allows you to specify the following for the migration source database backup that is restored for use during the upgrade:

- Enter the folder location (path) for the data files for the ICM/IPCC 7.5(1) database during a Technology Refresh migration on the destination server.

- Enter the folder location (path) for the transaction log files of the ICM/IPCC 7.5(1) database created during a Technology Refresh migration on the destination server.

While the Restore Location panel provides the defaults for the current SQL Server version, you may change these values.

Note:

- These paths must exist on the destination server or EDMT displays a dialog with an error.
- You can also **Browse** to the desired location for the data file or the log file.

In order for EDMT backup/restore with mapped drives to work properly, the SQL Server service (MSSQLSERVER) on the source machine needs to be set to "Log On" as an ICM domain/AD user with appropriate permissions instead of using the "LocalSystem" account. That same ICM domain/AD user needs to be a local administrator on the source machine and also needs read/write permissions to the backup share.

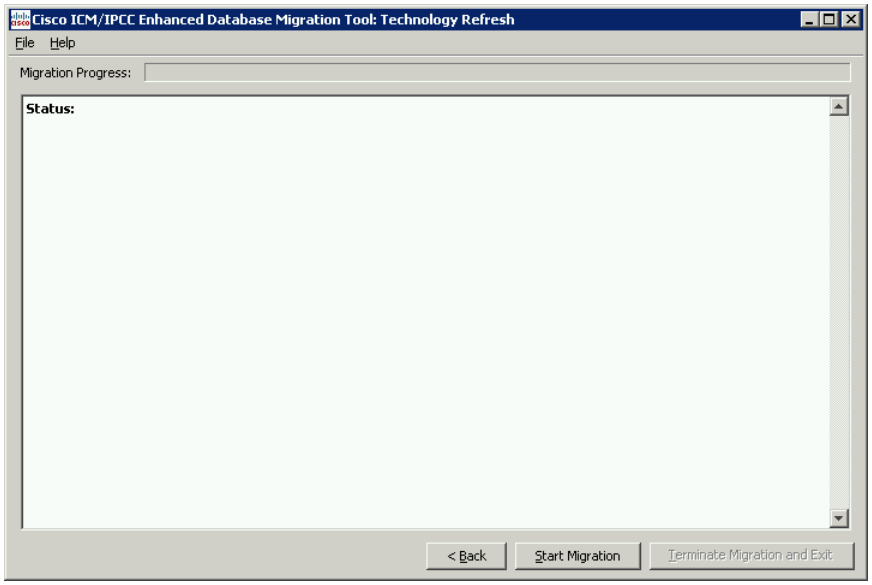
If you are backing up to a third box instead of the destination machine, then the destination machine needs to be setup in a similar fashion, for example: SQL Server service Log On as a domain user, the domain user is a local administrator, and has read/write permissions to the backup share.

Step 2 Complete the required information for the Backup Connection and the Destination Restore Location panels, then click **Next**.

The Migration Control dialog appears.

This EDMT panel allows you to start or terminate the data migration. It also displays the status of the data migration process.

Figure 12: EDMT TR Migration Progress Dialog - Before Starting Migration

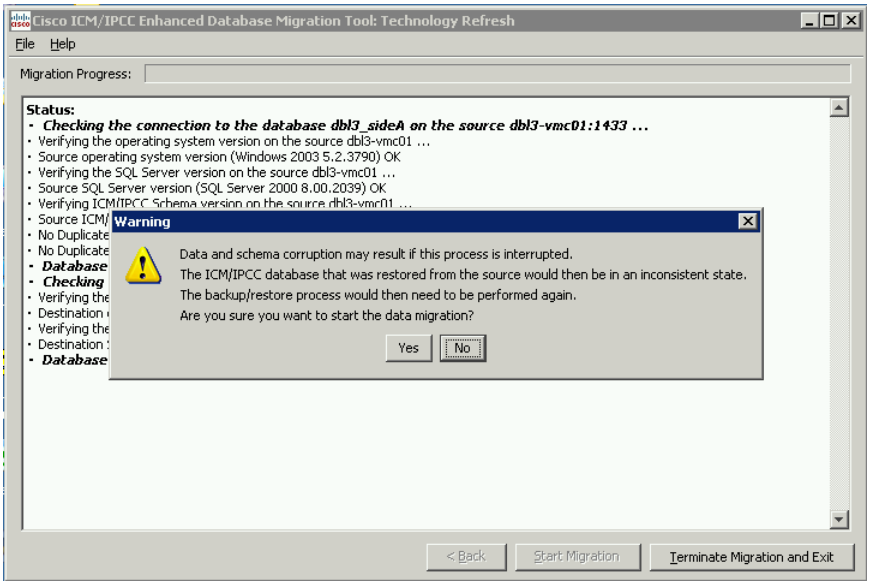


Refer to the Migration Control Dialog (page 74) for additional information on the Migration Control properties.

Step 3 Click **Start Migration** to begin the Technology Refresh database migration process.

The status of the migration process indicates that the database connection has been verified and a warning appears.

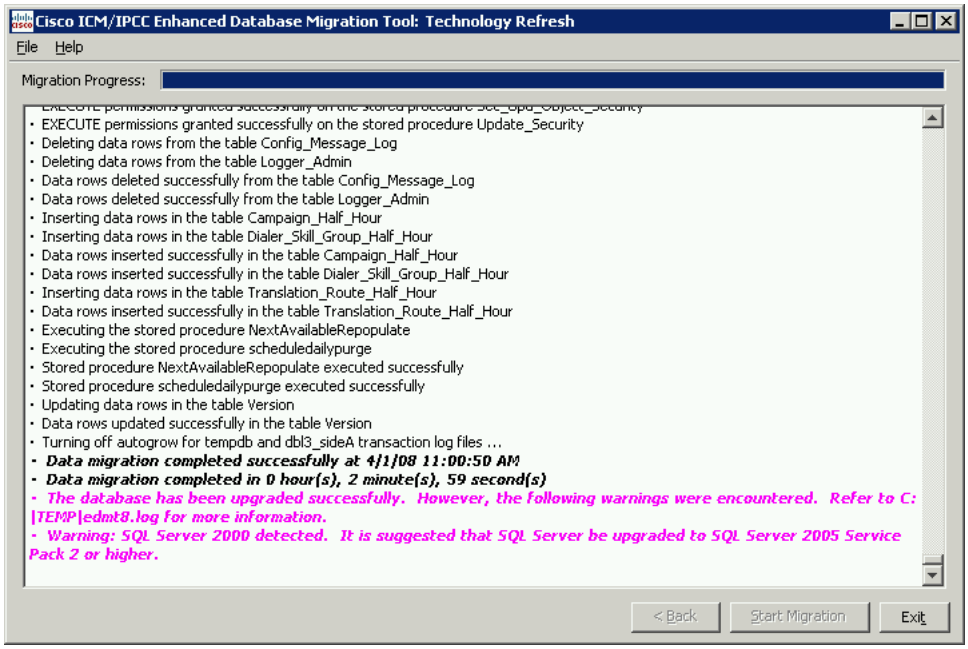
Figure 13: EDMT TR Migration Progress Dialog - After Starting Migration



Step 4 Click **Yes** and the Technology Refresh data migration begins.

The Migration Progress bar displays the progress of the migration while the Description field displays migration status messages.

Figure 14: EDMT TR Migration Progress Dialog - Migration Complete



Errors are displayed in bold, red, italic text.

Warnings are displayed in bold, magenta, italic text; and are repeated at the end of the migration as shown above.

Note: Warnings do not stop the migration process and the upgraded database is still usable. On the other hand, errors stop the migration process and leave the database in a corrupt state. You must restore the database from the backup you made prior to running EDMT if an error is encountered and you must run EDMT again after fixing whatever error is detected.

Step 5 Click **Exit** to close the EDMT.

EDMT Wizard Menus and Common Field(s)/Button(s)

File Menu

Option	Description
Exit	Selecting this menu option exits the EDMT application. It provides the same functionality as clicking the Windows **Close** button (X) or selecting **Alt-F4**. If the database migration is running, a warning appears informing you that you are interrupting the migration. • Click **Yes** to terminate the data migration and exit. • Click **No** (the default) to allow the migration to continue.

Help Menu

Option	Description
Help	Selecting this menu option activates the EDMT Help file in a new window. Keyboard shortcut: F1
About Cisco Unified ICM/CCE Enhanced Database Migration Tool	Selecting this menu option displays information about the application including the title, release, and copyright information.

Common Field(s)/Button(s)

Each EDMT panel contains one or more of the following common field(s) and/or button(s).

Field/Button	Description
Description field	Provides information about the displayed panel.
Back	Click to return to previous panel
Next	Click to advance to the next panel. **Note:** Once you click **Next** on the Migration Version/Type panel, the title of the application changes to add the type of migration. Thus, the title becomes either *"Cisco Unified ICM/CCE Enhanced Database Migration Tool: Common Ground"* or *"Cisco Unified ICM/CCE Enhanced Database Migration Tool: Technology Refresh"*.

Migration Version/Type Dialog

Migration Version Panel Properties

The Migration Version panel displays the Unified ICM/CCE release you are migrating from/to (upgrading an Unified ICM/CCE 7.0(x), 7.1(x), or 7.2(x) database to Unified ICM/CCE 8.0(1).

After all wizard panels are filled, EDMT retrieves the database version from the source database, and compares it to the schema versions for the Unified ICM releases supported for conversion. If the version detected is supported, the upgrade process continues.

If the schema version detected is not supported, an error message is displayed and the upgrade process does not continue. You must navigate back and select a database with the appropriate schema, or exit the program to terminate.

Migration Type Panel Properties

The Migration Type selected here affects the sequence of the EDMT wizard panels displayed as you progress through the rest of the migration process.

Radio Button	Description
Common Ground	Select to perform a Common Ground database migration.
Technology Refresh	Select to perform a Technology Refresh database migration.

Database Connection Dialog

Source Database Connection Panel Properties

Field/Button	Description
Host Name/IP Address	Enter the host name, or IP address, of the source server hosting the database (Logger or HDS).
Unified ICM/CCE Database Name (drop-down menu)	Enter the name of the Unified ICM/CCE 7.0(x), 7.1(x), or 7.2(x) source database from the drop-down menu.
SQL Server Port Number	Enter the TCP/IP port in which the source SQL Server is running. This field defaults to 1433, the standard SQL Server port, if you do not designate another port.
Authentication	Select SQL Server Authentication or Windows Authentication (the default) from the drop-down menu. **Note:** • When SQL Server Authentication is selected, enter a SQL Server username and password that is valid for the selected database. • When Windows Authentication is selected, the Domain Name, Username, and Password are disabled, and Windows Single Sign-On (SSO) uses your Windows authentication cached credentials to connect to the selected database.
Domain Name	Enter the domain name of the Windows account specified in the Windows Username field.
Username	Enter your Windows account user name to access the source database server. **Note:** Permissions to the master database, as well as to the Unified ICM database, are required. You must also have the permissions necessary to perform a database backup/restore. An account with SQL Server sysadmin privileges is sufficient.
Password	Enter the password for the user name entered in the Username field.

Destination Database Connection Panel Properties

Note: This panel only applies to Technology Refresh migrations.

Field/Button	Description
Host Name/IP Address	Disabled (read-only). The destination must be the current system.

Field/Button	Description
	For SQL Server Authentication, enter the host name, or IP address, of the destination server hosting the database (Logger or HDS).
Unified ICM/CCE Database Name (drop-down menu)	Disabled (read-only). The destination database will have the same name as the source database from the Source Database Connection Panel. When SQL Server Authentication is selected, enter the database name of the Unified ICM/CCE 7.0(x), 7.1(x), or 7.2(x) source server entered on the previous screen, from the drop-down menu. Unified ICM requires the database names to be the same.
SQL Server Port Number	Enter the TCP/IP port in which the destination SQL Server is running. This field defaults to 1433, the standard SQL Server port, if you do not designate another port.
Authentication	Select SQL Server Authentication or Windows Authentication (the default) from the drop-down menu. **Note:** • When SQL Server Authentication is selected, enter a SQL Server username and password that is valid for the selected database. • When Windows Authentication is selected, the Domain Name, Username, and Password are disabled, and Windows Single Sign-On (SSO) uses your Windows authentication cached credentials to connect to the selected database.
Domain Name	Disabled when Windows Authentication is selected. When SQL Server Authentication is selected, enter the domain name of the Windows account specified in the Username field.
Username	Disabled when Windows Authentication is selected. When SQL Server Authentication is selected, enter your Windows account user name to access the destination database server. **Note:** Permissions to the master database, as well as to the Unified ICM database are required. You must also have the permissions necessary to perform a database backup/restore. An account with SQL Server sysadmin privileges is sufficient.
Password	Enter the password for the user name entered in the Windows Username field.

Backup/Restore Dialog

Backup Connection Panel Properties

Field/Button	Description
Host Name/IP Address	Enter the host name, or IP address, of the server hosting the Windows share.

Field/Button	Description
	In most cases, this is the host name or IP address of the destination database server. This defaults to the destination database server, but it may be changed to point to another system.
Windows Share Name	Enter the name of the Windows share that is the location for the backup database file. **Note:** This could be a Windows administrative share (such as C$) or a different shared folder name.
Windows Share Domain	Enter the domain name of the Windows account specified in the Windows Username field. This is used for authentication when mounting the Windows Share.
Windows Share Username	Enter a Windows user name that has read/write permissions to the specified Windows share.
Windows Share Password	Enter the password for the user name entered in the Windows Share Username field.

Destination Restore Location Panel Properties

Field/Button	Description
Data Files Location	Enter the name of the directory where the database data file (.mdf) is to be created. The destination is prepopulated with the default location for database file storage for the version of SQL Server that you are running.
Log Files Location	Enter the name of the directory where the transation log file (.ldf) is to be created. The destination is prepopulated with the default location for database file storage for the version of SQL Server that you are running.
Browse	Alternate method to set the Data and/or Log Files locations.

Migration Control Dialog

Migration Control Dialog Properties

Field/Button	Description
Migration Progress	Indicates the completion status of the migration progress after **Start Migration** is selected. As each task of the database migration completes, the Migration Progress moves one bar. Some tasks take longer than others and this is reflected in the movement of the progress bar. **Note:** If an error occurs during the migration process, the Migration Progress bar changes from its standard color to red.
Status	When **Start Migration** is selected, the following warning message is displayed: **Warning:** ***Data and schema corruption may result if this process is interrupted. The system database that was restored from the source would***

Field/Button	Description
	then be in an inconsistent state. The backup/restore process would then need to be performed again. Are you sure you want to start the data migration? Click **No** to abort the migration. Click **Yes** to start the data migration. This field then displays each task of the migration process as it starts and finishes. It also indicates when the migration process started, ended, and how long it took. Each message in the Status field is logged. Errors are displayed in bold, italic, red text. Warnings are displayed in bold, italic, magenta text; and are repeated at the end of the migration. **Note:** Warnings do not stop the migration process. Errors stop the migration process and may leave the database in a corrupt state. The EDMT logs directory is located in the TEMP directory on the Windows system drive (typically C:\TEMP). The active log file is called c:\temp\edmt8.log.
Start Migration	This button tests the entered database connection values by attempting to access the database(s). All of the connection information was checked for validity when entered on its respective panels. The connections check reports whether the database connections were made or not in the migration Status field. A successful source database connection result is indicated by the following Status messages: **Status:** **Checking the connection to the database dd1_sideA on <source hostname>:<source port> ...** Displays miscellaneous messages ..... **Database connection to the source verified OK** A successful destination database connection result is indicated by the following Status messages: **Status:** **Checking the connection to the database dd1_sideA on the destination <destination server> ...** Displays miscellaneous messages ..... **Database connection to the destination verified OK** **Verifying the source SQL Server and destination SQL Server using the same collation ...** **Both source and destination SQL Servers using the same collation (Latin1_General_BIN)**

Field/Button	Description
	If a problem occurs, go back to the appropriate panel and change the incorrect information. If the connections check passes, the database migration process starts.
Terminate Migration and Exit	Disabled until the migration process starts. When selected, the following warning is displayed: **Warning:** ***Data and schema corruption may result if this process is interrupted. The system database would then be in an inconsistent state. The backup/restore process would then need to be performed again. Are you sure you want to terminate the data migration?*** Click **No** to continue migration. Click**Yes** to terminate migration and exit the tool. Once the database conversion process starts, you may interrupt the process by selecting **Cancel**. Cancelling the database conversion process causes the database to be in an inconsistent state. If this happens, you must perform the following : 1. Restore the database that you backed up prior to running EDMT, to put the database back into a consistent state. 2. Rerun EDMT. **Note:** If you terminate the data migration, you must restore the database from the backup using the overwrite option.

How to start the data migration process

Step 1 Click **Start Migration**.

The following warning appears:

Warning: ***Data and schema corruption may result if this process is interrupted. The Unified ICM/CCE database that was restored from the source would then be in an inconsistent state. The backup/restore process would then need to be performed again. Are you sure you want to start the data migration? Click* No *to abort the data migration. Click* Yes *to start the data migration.***

This field then displays each task of the migration process as it starts and finishes. It also indicates when the migration process started, ended, and how long it took.

Each message in the Status field is logged. Errors shown in this field are presented in bold italic red text. The EDMT logs directory is located in the TEMP directory on the Windows system drive (typically C:\TEMP).

Step 2 Select the appropriate option.

How to terminate the in-progress data migration

If it becomes necessary to terminate an in-progress data migration, perform the following.

Step 1 Click **Terminate Migration and Exit**.

The following warning appears:

Warning: ***Data and schema corruption may result if this process is interrupted. The Unified ICM/CCE database would then be in an inconsistent state and need to be restored from backup. Are you sure you want to terminate the data migration? Click* Yes *to terminate the migration process and exit the application. Click* No *to continue the migration process.***

Step 2 Select the appropriate option.

If you terminate the migration, you must then perform the following:

- Drop the database restored on the destination server.
- Rerun EDMT.

Chapter 8

Service Account Manager

ICM and Contact Center Enterprise services, such as Logger or Distributor, execute under the context of a domain user account commonly known as a service account. ICM Setup and System IPCC Installer create these service accounts in the Active Directory (AD) domain and associate them with the corresponding service on the ICM server.

The Service Account Manager is invoked by ICM Setup or System IPCC Installer when you choose to manipulate the default service account creation process.

The Service Account Manager decouples the service account management from ICM Setup or System IPCC Installer. This provides you with the needed flexibility to:

- either create a new service account or choose one created prior to ICM Setup or System IPCC Installer.
- enter your own password or let the ICM application generate one for you.

  Note: If passwords are changed using an application other than SAM, SAM cannot detect the changes.

- allow you (when applicable) to choose whether or not to update the account in AD and use existing AD accounts as ICM service accounts.
- allow you to fix service account group membership issues (such as modifying ICM service account passwords) without recreating accounts or without re-running ICM Setup or System IPCC Installer.

The Service Account Manager is called by ICM Setup or System IPCC Installer to when either Creating Service accounts or Use existing accounts checkboxes is selected. When Creating Service Accounts checkbox is selected, the Setup/Installer silently calls SAM to generated Account and password. When the Use existing account checkbox is selected, Setup/Installer calls SAM and the graphical interface.

The Service Account Manager provides an additional functionality via its command line interface to set service account memberships for CICR replication in a NAM/CICM deployment.

You have the option to re-run the Service Account Manager post ICM/System IPCC installion to modify the ICM service account, or its password, or to verify the account health. The Service Account Manager must be executed on each server locally to configure the service accounts for services listed below.

The Service Account Manager is limited to function only with the following services:

- Distributor
- LoggerA
- LoggerB
- Tomcat
- Jaguar

This chapter contains the following topics:

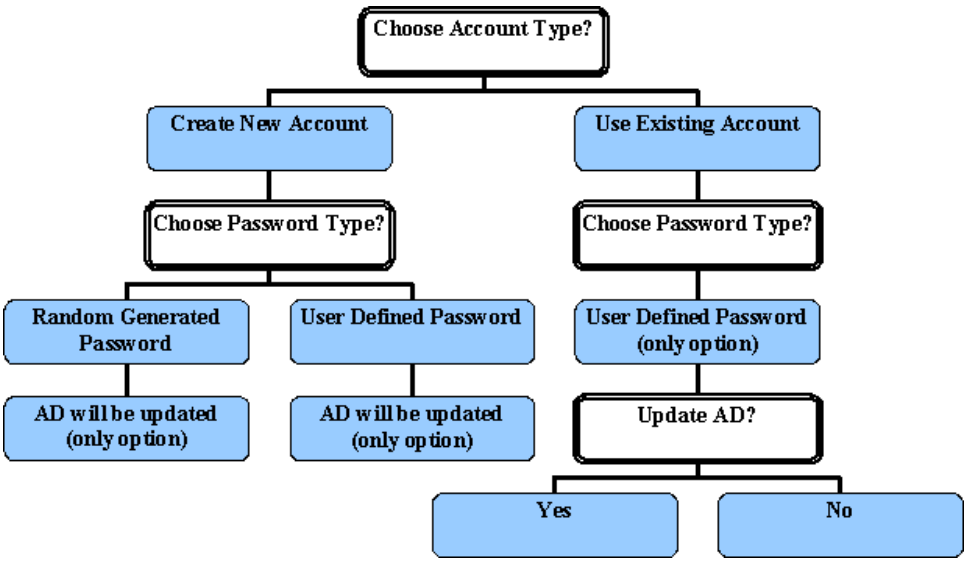
Managing Service Accounts

The Service Account Manager serves three purposes. It allows you to:

1. create new accounts with random passwords, like the current ICM Setup and System IPCC Installer.
2. use existing AD accounts as ICM service accounts.
3. Provide an interface to modify ICM service account passwords.

The following diagram illustrates the basic workflow of the Service Account Manager.

Figure 15: Service Account Manager Application Workflow



Integration with ICM Setup and System IPCC Installer and Upgrade

Currently ICM Setup and System IPCC Installer create a service account in AD for the following ICM services and then associate these services with their respective service accounts:

- Distributor
- Logger
- Tomcat
- Jaguar

ICM Setup and System IPCC Installer are modified to create the above listed services using the NetworkService account, a Windows predefined local account (other services such as Router and PG are not modified).

Note: You must have Microsoft .NET Framework 3.5 installed on all systems you intend to install the Service Account Manager on. This is automaticallt installed by ICM Setup or the System IPCC Installer.

ICM Setup and System IPCC Installer use the Service Account Manager to create the service accounts. You can choose to either let Setup/Installer manage the service account creation process, or take control over the service account management process.

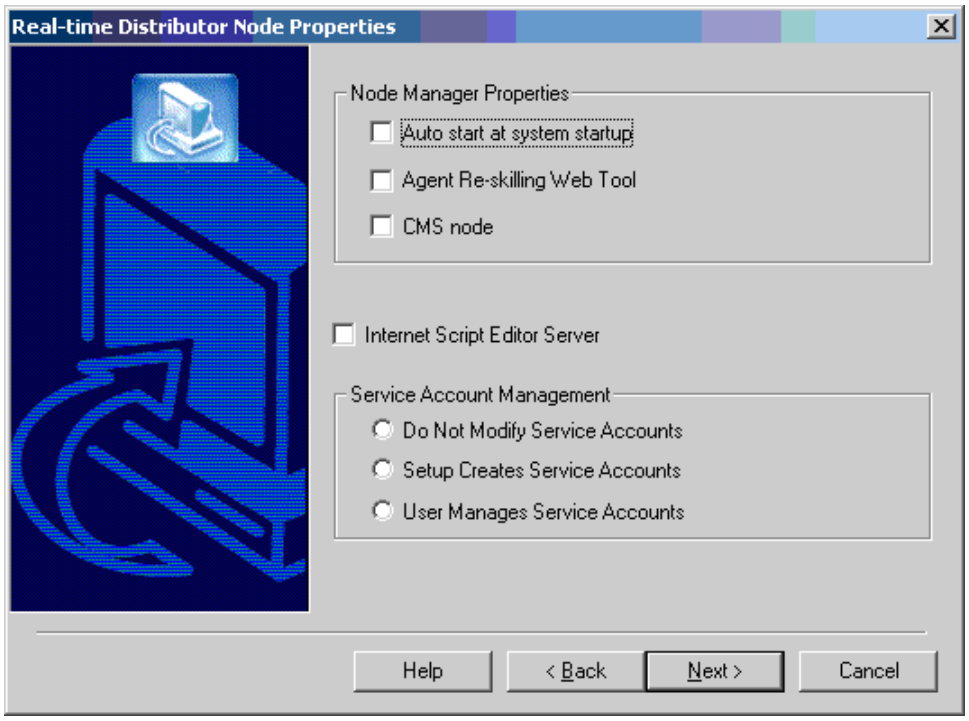
Interaction with ICM Setup

.

The following ICM Setup dialogs have been modified (the **Recreate Service Account** checkbox has been removed and the **Service Account Management** section has been added) to gather service account management input:

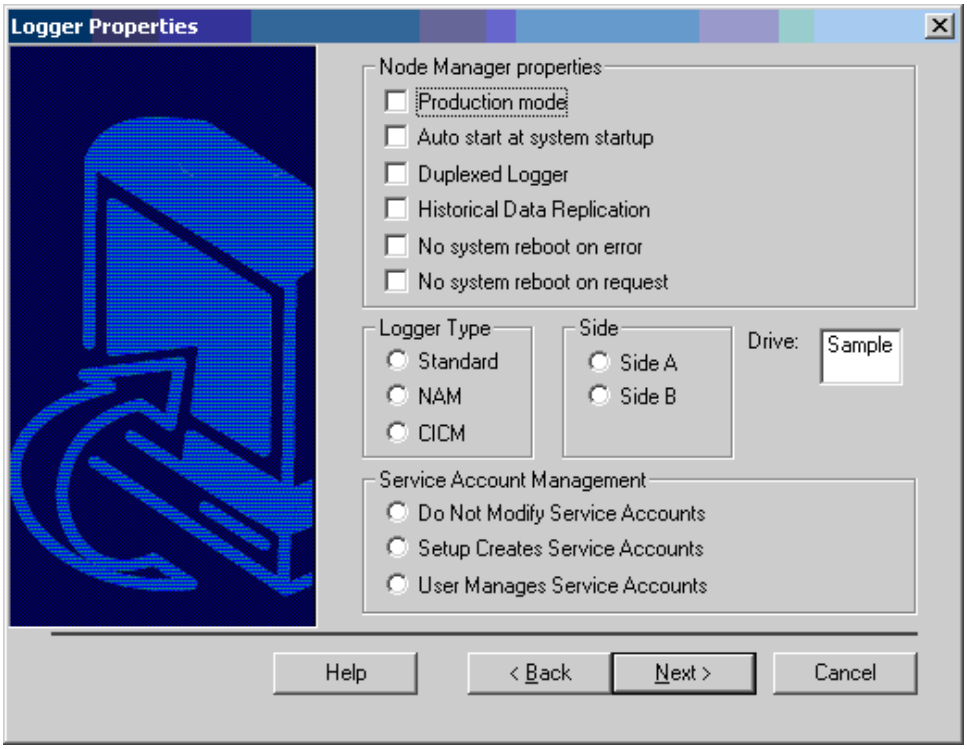
- Distributor

Figure 16: Distibutor Setup Dialog



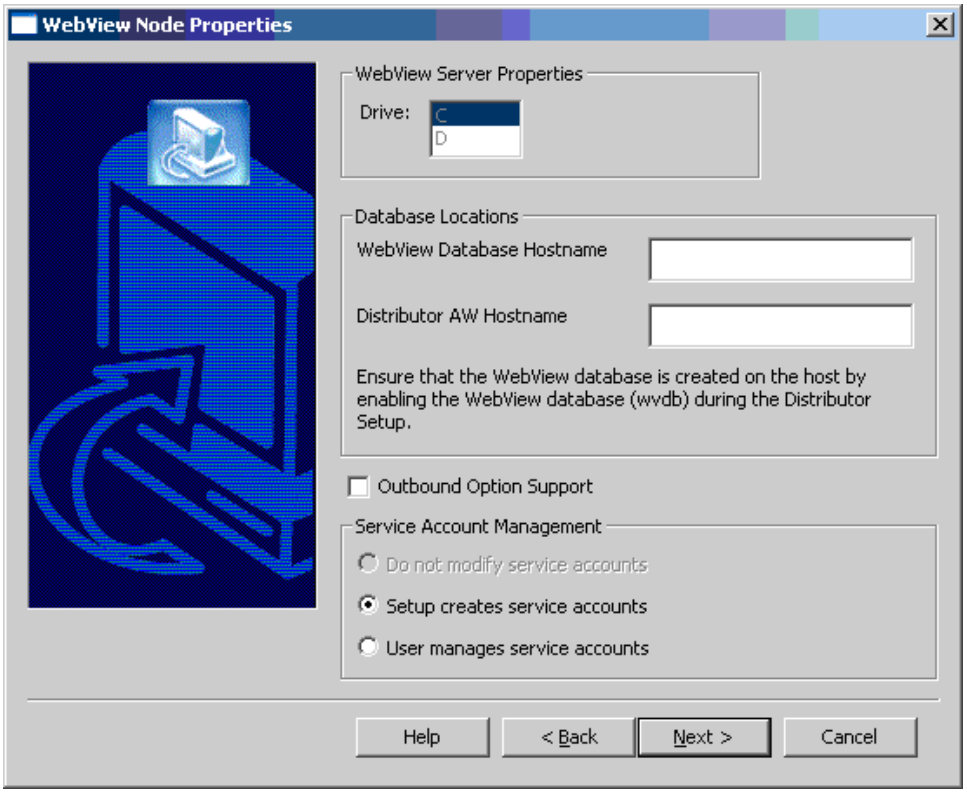
- Logger

Figure 17: Logger Setup Dialog



- WebView

Figure 18: WebView Setup Dialog



The **Service Account Management** section contains three radio buttons:

- Do not modify service accounts
- Setup creates service accounts
- User manages service accounts

Additional information concerning the three new radio buttons can be found in the following sections.

Fresh Installation using ICM Setup

During a fresh installation of the Logger, Distributor, and/or WebView component(s), **Do not modify service accounts** is grayed out and **Setup creates service accounts** is selected by default. You must choose between **Setup creates service accounts** and **User manages service accounts**. When you click **Next**, Setup notes your selection. Setup then creates the service(s) using the NetworkService account. After creating the service(s), Setup invokes the Service Account Manager as follows:

- If you selected **Setup creates service accounts**, Setup invokes the Service Account Manager silently, without bringing up the Service Account Manager user interface.
- If you selected **User manages service accounts**, Setup invokes the Service Account Manager to allow you to take control of setting up the service account name and password.

Editing Component using ICM Setup

If you edit any of the three components listed above, **Do not modify service accounts** is enabled and selected by default.

Upgrade using ICM Setup

During an upgrade, once **Upgrade All** is selected, there is no other user interface. You have no options regarding service account creation. ICM Setup uses the following logic to decide if Service Account Manager needs to be invoked on not:

- *Common Ground*

  If the services already exist, ICM upgrade does not modify the service accounts.

- *Technology Refresh*

  ICM Upgrade invokes Service Account Manager to create the service accounts.

Interaction with the System IPCC Installer

Fresh Installation of System IPCC

Service Account Management has been added to the System IPCC Installer. It has the following two radio buttons:

- Installer Creates Service Accounts
- User manages service accounts

Similar to ICM Setup, the default selection for a new installation is **Installer Creates Service Accounts**. When you choose between the two, the Installer takes note of your selection, then acts on it later. The Installer lays down the files, updates the registries, and creates the Distributor, Logger, WebView, and Tomcat services using the NetworkServices account. The Installer then calls the IPCC Machine Initializer to create the ICM OU, the facility and the instance OU.

The Installer passes a new argument to the IPCC Machine Initializer indicating your choice of service account management. The IPCC Machine Initializer creates the OU and security groups. Then, if you selected **Installer Creates Service Accounts**, after the successful installation, the IPCC Machine Initializer tool invokes the Service Account Manager silently, without bringing up the Service Account Manager UI, and then passes control back to the System IPCC Installer.

If you selected **User manages service accounts**, after the successful installation, the IPCC Machine Initializer tool invokes the Service Account Manager for you to take control of setting up the service account name and password. Once the Service Account Manager is closed, the IPCC Machine Initializer tool passes the control back to the Installer.

If IPCC Machine Initializer tool fails then the Service Account Manager is not invoked, no matter what option is selected by you regarding service account creation. Fix the issue as reported by the IPCC Machine Initializer and then rerun the IPCC Machine Initializer in standalone mode. This, in turn, runs Service Account Manager as explained in the *Standalone Use of the IPCC Machine Initializer* section, following.

Upgrade of System IPCC

A new dialog panel has been added to the System IPCC Upgrade, with the following radio buttons:

- **Do not modify service accounts**
- **Setup creates service accounts**
- **User manages service accounts**

Similar to ICM Upgrade, the default selection is **Do not modify service accounts**.

When performing an System IPCC *Common Ground Upgrade*:

- System IPCC Upgrade does not invoke the IPCC Machine Initializer. Unlike System IPCC Installer, System IPCC Upgrade invokes the Service Account Manager directly when needed.
- If you select **Do not modify service accounts**, the service accounts are not recreated and Service Account Manager is not invoked.
- If you select **Installer Creates Service Accounts**, System IPCC upgrade invokes the Service Account Manager tool silently, without bringing up the Service Account Manager.
- If you select **User manages service accounts**, System IPCC Installer invokes the Service Account Manager tool, allowing you to take control of setting up the service account name and password. Once the tool is closed, System IPCC upgrade takes control and finishes the installation steps.

When performing an System IPCC *Technology Refresh Upgrade*:

- System IPCC Upgrade invokes the IPCC Machine Initializer. This is the only difference from the System IPCC Common Ground Upgrade above.

Standalone Use of the IPCC Machine Initializer

The IPCC Machine Initializer can be run as a standalone application to create or modify the facility OU. When creating/modifying the facility OU, the initializer invokes the Service Account Manager automatically. If the facility OU is changed, the service accounts must be recreated.

WebView configuration

Both ICM Setup and System IPCC Installer configure Jaguar service as a part of the installation. However, Jaguar service cannot be configured unless a service account is associated with it. Since service accounts are no longer created by Setup, Setup cannot configure the Jaguar service. Due to this, the Service Account Manger is responsible for configuring the Jaguar service after associating a service account with it.

Other Considerations

Permissions

You must have the correct privileges to create or modify accounts in the domain. Typically, this action is performed by a domain administrator. However, the Service Account Manager does not enforce domain administrator privileges. You are expected to have the right permissions before invoking the Service Account Manager.

Domain Restriction

The service account must be in the same domain as the ICM server. When choosing an existing account, the Service Account Manager restricts the account to be selected from the same domain as the server.

Special Case: When the distributor is in a different domain than the logger, the distributor service account must be placed in the instance service security groups of both its own domain and the logger domain. While this functionality was originally taken care of by Setup, this function is now handled by the Service Account Manager.

AD Update Failures

If the Service Account Manager finds that a service is running, it first requests your permission, then if you approve, it stops the service. If you choose not to stop the service, the Service Account Manager does not modify the service account information. The Service Account Manager automatically starts the service if it had explicitly stopped the service prior to editing the account information. If the Service Account Manager fails to update the account in AD, due to either a noncompliant password policy or any connectivity error, the Service Account Manager warns you and logs the error. At that point, you can choose to fix the problem and retry, or cancel.

Logging

The application maintains its own log file, when invoked as a standalone application. If called through Setup/Installer, logs are written to the Setup/Installer log files only.

Set Service Account Memberships for CICR Replication

When upgrading the Cisco Intelligent Contact Manager (ICM) Hosted Edition to ICM 7.0 (or later) the CICR replication process (CRPL) does not have the proper rights and permissions in order to make configuration updates to the customer instances (CICM) and the slave NAM instance without manually configuring Active Directory.

This configuration entails adding the Provisioning NAMÃƒÂ¢Ã¢â€šÂ¬Ã¢â€ Â¢s logger service accounts to the service groups of the CICMs and the slave NAM. This way the Provisioning NAMÃƒÂ¢Ã¢â€šÂ¬Ã¢â€ Â¢s service account has the permissions necessary to update the databases of the CICM and the slave NAM.

One function the Service Account Manager provides is to automate the manual configuration steps (described at: http://www.cisco.com/en/US/products/sw/custcosw/ps5053/products_tech_note09186a00806c6609.shtml). This functionality is exposed through the Service Account Manager command-line interface as described in the *Set Service Account Memberships for CICR Replication* section.

Typically this functionality is utilized through two batch files (one for the A side and the other for the B side) where there is an entry for each CICM or slave NAM as a destination (/Dest). Each time ICM Setup is executed, running the batch file follows to configure the Active Directory permissions properly.

Service Account Manager End User Interfaces

The Service Account Manager has two user interfaces:

- The Graphical User Interface (page 88) consisting of the following dialogs:
  - Main Dialog (page 88)
  - Edit Service Account Dialog (page 89)
- The Command Line Interface (page 95)

Service Account Manager Graphical User Interface Dialogs

A shortcut to the application can be found in Windows Start > Programs folder.

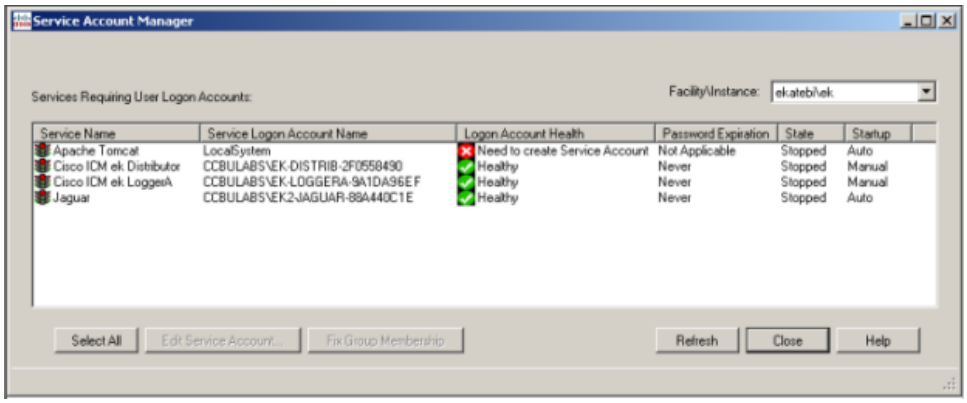
- For ICM, the shortcut is under ICM Administration.
- For System IPCC, the shortcut is under IPCC Administrator.

The Service Account Manager has two dialogs

- The Main dialog

  Lists all services with their account information.

  Figure 19: Main Service Account Manager Dialog

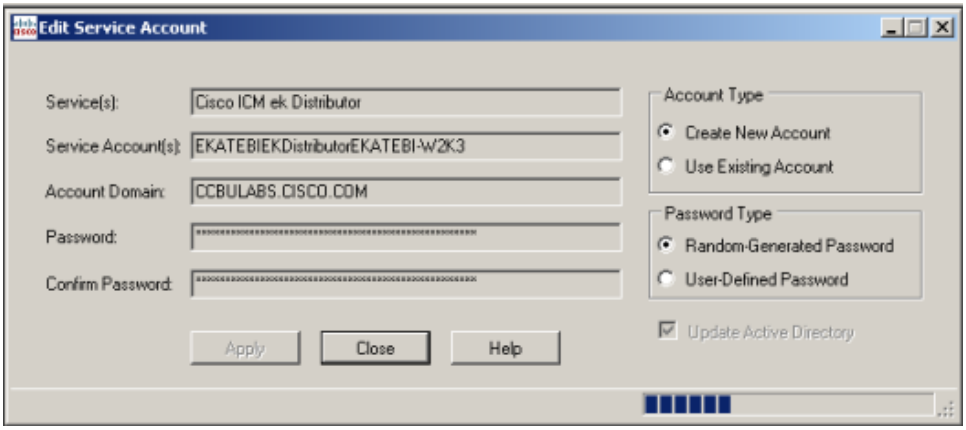


  Note: For additional information on all dialog fields and buttons refer to Service Account Manager - Main Dialog (page 88).

- The Edit Service Account dialog

  Used to edit the service account information.

Figure 20: Service Account Manager - Edit Service Account Dialog



Note: For additional information on all dialog fields and buttons refer to Service Account Manager - Edit Service Account Dialog (page 89).

Service Account Manager - Main Dialog

The Service Account Manager can be used as a standalone application as well as being invoked from ICM Setup and System IPCC Installer.

The Main Service Account Manager dialog is the application's primary interface. It consists of the *Services Requiring User Logon Accounts* section (which contains the *Service Name*, *Service Logon Account Name*, *Logon Account Health*, *Password Expiration*, *State*, and *Startup* fields), the **Facility/Instance** dropdown; and the **Select All**, **Edit Service Account**, **Fix Group Membership**, **Refresh**, **Close**, and **Help** buttons.

The following table provides a description for each of the fields and buttons for this dialog.

Field/Button/ Dropdown	Description
Service Name	A list of all relevant services. If there are no relevant services on the server, such as a Distributor, TomCat, Jaguar, or Logger; the field displays the message "This instance does not have any service that requires a service account."
Service Logon Account Name	Displays the service account name for the list of relevant services.
Logon Account Health	The Service Account Manager has an account health check mechanism. When the application starts, it scans all relevant ICM services and flags them as indicated below. • Green – Healthy Account: the service account state is normal. • Yellow

Field/Button/ Dropdown	Description
	– Password Warning: the password is due to expire in less than 7 days. • Red – *Invalid Account*: service has an invalid account associated with it. – *Password Expired*: service account password has expired. – *Group Membership Missing*: service account is missing from the required domain or local security groups. – *Account not associated with service*: service account created but not replicated, hence not associated yet. The following messages could appear in the Health column. • Healthy – Only applies to the service account, not the service itself. – The account is a member of the required ICM security groups. – The account has been validated to start a service. – If the account password is changed outside of the Service Account Manager application, *Healthy* would be displayed even though the service may not actually be healthy because this application cannot detect the change. • Need to create service account – The Service Account Manager must be used to create a service account for each service. • Account not in Instance Domain – The Service Account Manager is capable of detecting whether or not a service account exists in the ICM or System IPCC domain. • Account Disabled

Field/Button/ Dropdown	Description
	– In AD an account can be enabled or disabled. This message indicates the account is disabled in the domain. • Password Expired • Account not a member of the Instance Service Group • Service Group not a member of local Administrators group • Central Controller (sideA) Domain name is unknown (Distributor only) – Distributors can be in a different domain than the Central Controller. When **Fixed Group** is selected, you will be queried for the domain name of the Central Controller if it is different than that of the Distributor. • Central Controller (sideA) Domain is not trusted or trust is not two-way (Distributor only) – There must be a two-way trust between the Central Controller and the Disributor. SAM detects the lack of the trust relationship and displays this message. SAM may detect this issue, but is unable to fix it. • Account not a member of LoggerA Domain Service Group (Distributor only) – If the Distributor is on a different domain than the Central Controller, it applies the Distributor's Domain Service Group to both itself and the Central Controller. • Central Controller (sideB) Domain name is unknown (Distributor only) – Distributors can be in a different domain than the Central Controller. When **Fixed Group** is selected, you will be queried for the domain name of the Central Controller if it is different than that of the Distributor. • Central Controller (sideB) Domain is not trusted or trust is not two-way (Distributor only) – There must be a two-way trust between the Central Controller and the Disributor. SAM detects the lack of the trust relationship and displays this message. SAM may detect this issue, but is unable to fix it.

Field/Button/ Dropdown	Description
	• Account not a member of LoggerB Domain Service Group (Distributor only) – If the Distributor is on a different domain than the Central Controller, it applies the Distributor's Domain Service Group to both itself and the Central Controller. • Account not associated with service – When SAM associates an account with a service it may run into replication issues. Use **Edit** and select **Associate the account with a service** rather than selecting editing from the beginning. • Service not validated for starting – When SAM validates a service it may run into replication issues. Use **Validate** to successfully start the service. • EAServer configuration for WebView failed (Jaguar only) – After an account is associated with the Jaguar service and validated SAM attempts to run a script to configure WebView. If that script fails, this message appears. • Password About To Expire – Check the **Password Expiration** field to determine how long before the password expires. The Service Account Manager can then be used to reset the password for this pre-existing account. A service has an *Invalid Account* health state immediately after creation since no domain account is assigned to it yet. This is expected behavior. A service can have a *Missing Group Membership* problem due to a prior AD related failure. The Service Account Manager is capable of fixing this issue by providing an interface to reattempt placing the account in the relevant local and domain security groups. **Note:** SAM health reporting may be inaccurate for the period of time while AD replication is in progress. The previous health state may be indicated during this time.

Field/Button/ Dropdown	Description
Password Expiration	Service account passwords created by the Service Account Manager are set to not expire. However, you do have the option of setting the service account passwords to expire. **Note:** • Any service with an account password that expires in seven (7) days is yellow flagged by the application. • You own the responsibility to refresh the passwords before they expire. If you do not, the ICM services fail to function.
State	The current stateof the service (Stopped, Start/Stop Pending, or Running).
Startup	Displays how the service is started (Manual or Automatic).
Facility/Instance	Dropdown displaying the "Facility/Instance" name. In case of multiple instances, the default "Facility/Instance" selected in the dropdown is the last instance edited by Setup. Select a specific instance. The Service Account Manager lists all relevant services with their account information, account health, password expiration and startup state for the selected instance. If there are no relevant services on the server (such as a Distributor, TomCat, Jaguar, or Logger) the Service Account Manager displays the message: *This instance does not have any service that requires a service account.*
Select All	Click to select all listed services.
Edit Service Account	To fix any account issues, edit one, a few, or all accounts at the same time by selecting them and clicking this button. Once in the dialog, the Service Account Manager prompts you to try to use the account recently created, as it keeps a track of it. If you agree to use the recently created account, the application tries to reuse the previously created account, thereby escaping from the recursive cycle of trying to create and use an account. If you chose random password, the application creates a new one, or prompts you to enter one. The application never stores the password.
Fix Group Membership	Available ONLY if an account with the *Group Membership Missing* health state is selected.
Refresh	Refreshes all information in the Service Account Manager Main dialog.
Close	Closes the Service Account Manager dialog.

Field/Button/ Dropdown	Description
Help	Select to access the online help for the Service Account Manager.

Service Account Manager - Edit Service Account Dialog

The Edit Service Account dialog allows you to create a new or use an existing account, and to choose a random or a user defined password. The status bar at the bottom of the dialog displays status messages as needed.

The following table provides a description for each of the fields, buttons, and checkboxes for this dialog.

Field/Button/Checkbox	Description
Services	Displays the name of the service to be edited.
Service account(s)	Displays the account name for the selected service.
Account Domain	Displays the server's domain. (Read Only)
Password	If the Password Type selected is **Random-Generated Password**, this field is populated with the generated password. If the Password Type selected is **User-Defined Password**, enter the password to be used for this account.
Confirm Password	If the Password Type selected is **Random-Generated Password**, this field is populated with the same generated password as the Password field. If the Password Type selected is **User-Defined Password**, re-enter the password to be used for this account.
Account Type	Allows you to either create a new account or use an existing account by selecting the appropriate radio button. **Create New Account** is the default if there is no domain account assigned yet. **Use Existing Account** is the default if a domain account is already assigned.
Password Type	Allows you to choose a random-generated or a user-defined password by selecting the appropriate radio button. **Random Generated Password** is the default if you are creating a new account. **User Defined Password** is the default, and only, option when using an existing account.

Field/Button/Checkbox	Description
Update Active Directory	**Checked** is the default, and only, option if you are creating a new account. **Note:** By checking this checkbox, you are actually making changes to the Active Directory domain and any changes to passwords will effect the password of the existing user. **Unchecked** is the default if using an existing account.
Apply	Click to apply any changes on this dialog.
Close	Click to close this dialog. Whenever this dialog is closed, the Service Account Manager determines if a valid domain account is associated with the service(s) or not. If the Service Account Manager finds that the you did not successfully associate a valid domain account with a service, it warns you that the service will fail to function until you use the Service Account Manager to associate a valid domain account with the service.
Help	Select to access the online help for the Service Account Manager.

Service Account Manager - Command Line Interface

Note: The Service Account Manager command line option is only supported for NAM/CICM replication.

Creating Default Service Accounts Silently

The command line interface is used by ICM or System IPCC Setup to silently create service accounts.

Setup passes the following three arguments to the Service Account Manager:

/Instance <InstanceName>

- The InstanceName argument specifies the ICM instance name for which the service is being setup.

/Service <ServiceType>

- The Service argument specifies the type of the service whose account name and password are being created.

  For example: /Service Distributor

Service types to be used are:

– Distributor

– LoggerA -- For use when on Side A of the logger or for All-In-1 ICM/CCE

– LoggerB -- For use when on Side B of the logger only

– Tomcat

– Jaguar

/Log <Path\LogFileName>

- The Log argument specifies the log file name and the path where the log is appended. Typically, ICM Setup and System IPCC Installer passes their own log file name to append the logs. The Service Account Manager also maintains its own log file in the temp folder.

Note:

- If any one of the arguments is missing or incorrect, the Service Account Manager returns an error to Setup.
- If Setup needs to create accounts for more than one service, it invokes the Service Account Manager multiple times using the command line interface.

Setting Service Account Memberships for NAM/CICM Replication

When the application is invoked from the provisioning NAM's Logger servers (sides A and B), the command line is as follows:

- ServiceAccountManager
- /SrcInstance<InstanceName>
- /DestDomain<DomainName>
- /DestFacility<FacilityName>
- /DestInstance<InstanceName>

Service Account Manager - How to ...

How to create a new account for a single service

Step 1 Select a single service from Main Service Account Manager dialog.

Step 2 Click **Edit Service Account**.

The Edit Service Account dialog opens.

Step 3 Select **Create New Account**.

If no domain account is associated with the service then **Create New Account** is selected by default.

Step 4 Enter a password or have one generated randomly.

Random-Generated Password is selected by default.

Step 5 Click **Apply**.

The Service Account Manager creates a new account in AD with a password.

If the account name already exists, the Service Account Manager asks you to either recreate it, or just update the password.

The application associates the account with the service on the server. It places the account in the required domain security group and local security group, and sets the required permissions. Service account gets recreated, or just the password changes, based on your selection prior to clicking **Apply**.

Note: If the Service Account Manager fails to put the account in domain security group, it asks you to rerun the application 20 minutes later to give AD time to replicate the account.

How to update an existing account for a single service

Step 1 Select a single service from Main Service Account Manager dialog.

Step 2 Click **Edit Service Account**.

The Edit Service Account dialog opens.

Step 3 Select **Use Existing Account**.

If a domain account is associated with the service, **Use Existing Account** is selected by default.

Step 4 Enter a password.

Step 5 Choose whether or not to update the password in AD.

Step 6 Click **Apply**.

If previously selected, the Service Account Manager updates the password in AD. It updates the service on the server with the new account information.

The Service Account Manager then places the account in required domain security group and local security group, and sets the required permissions.

Note: If the Service Account Manager fails to put the account in domain security group, the application asks you to rerun the application 20 minutes later to give AD time to replicate the account.

How to create new accounts for more than one service

Step 1 Select multiple services or click **Select All**.

Note: Use the normal Windows conventions for selecting all or multiple services.

Step 2 Click **Edit Service Account**.

The Edit Service Account dialog opens.

The Service Name column lists all services. Since multiple services are selected, **Use Existing Account** is selected by default.

Step 3 Click **Create New Account**.

A separate service account is created for each service.

Step 4 Enter a password, or have one generated randomly.

If you chooses to enter password, then the same password is shared across all accounts.

If you choose to randomize the password, a separate random password is generated for each account.

Step 5 Click **Apply**.

The Service Account Manager creates multiple accounts in AD with the password. The application associates each account with the respective service on the server. It places the accounts in the required domain security group and local security group, and sets the required permissions.

Note: If the Service Account Manager fails to put the account in domain security group, it asks you to rerun the application 20 minutes later to give AD time to replicate the account.

How to update an existing account for more than one service

Step 1 Select multiple services or click **Select All** on the Main Service Account Manager dialog.

Step 2 Click **Edit Service Account**.

The Edit Service Account dialog opens.

The Service Name column lists all services. Since multiple services are selected, **Use Existing Account** is selected by default.

Step 3 Enter an account name.

Step 4 Enter a password.

Step 5 Choose whether or not to update the password in AD.

Step 6 Click **Apply**.

If previously selected, the Service Account Manager updates the password in AD. It updates the service on the server with the new account information.

The Service Account Manager then places the account in required domain security group and local security group, and sets the required permissions.

Note: If the Service Account Manager fails to put the account in domain security group, the application asks you to rerun the application 20 minutes later to give AD time to replicate the account.

How to fix the group membership issue of one or more accounts in the "Group Membership Missing" health state

Fix Group Membership is only enabled when account(s) in the "Group Membership Missing" health state is (are) selected.

Step 1 Select the unhealthy account(s) displaying the "Group Membership Missing" state.

Step 2 Click **Fix Group Membership**.

If any of the selected account(s) is/are not in the "Group Membership Missing" state, **Fix Group Membership** is disabled.

Step 3 Click **Apply**.

The Service Account Manager then places the account in required domain security group and local security group, and sets the required permissions.

Note: If the Service Account Manager fails to place the account(s) in the groups, it provides the appropriate error.

Service Account Manager - How to ...

Chapter 9

Upgrade Procedures

Determine which of the following upgrade examples is similar to your system. Follow the procedures for each step indicated in the Reference column.

Warning: In order to complete an upgrade successfully, the order of upgrade as defined in this guide MUST be followed.

Warning: When upgrading an ICM/IPCC parent/child system, upgrade the child first, then the parent. This prevents issues in case of a protocol change.

This chapter contains the following topics:

Technology Refresh Upgrade Examples

Before undertaking a TR upgrade, it's important that the newly deployed servers be installed. The Active Directory environment (whether corporate or dedicated to the ICM/IPCC applications) must be configured/staged. The Windows Firewall configuration scripts must be deployed before ICM/IPCC servers can accept network connections.

Note: For addition Windows and SQL Server staging information, refer to the **Staging Guide, ICM/IPCC Enterprise/Hosted, ICM/IPCC Software Release 7.x(y)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_installation_guides_list.html)

Two technology refresh examples are provided below. Both examples assume redundant configurations with Side A and Side B Routers and Loggers, and that Side A and Side B HDS/Distributor AWs are part of the system being upgraded and are required to support the number of reporting users. The examples therefore include the deployment of a temporary HDS/Distributor AW to maintain maximum system functionality and reporting capacity during

the upgrade process. The deployment of a temporary HDS/Distributor AW may not be necessary depending on the contact center hours of operation, the estimated upgrade time for each ICM/IPCC node (for additional information refer to Chapter 5: ICM/IPCC 7.5(1) Upgrade Time and Space Requirements (page 29)), whether one or two HDS/Distributor AWs are deployed, the reporting user capacity required during upgrade, and other operational factors. The temporary HDS/Distributor AW does not provide historical reporting, only real-time reporting is provided. Both examples assume Side A is upgraded first, although the B side can be upgraded first.

Technology Refresh Example 1: Production HDS/Distributor AW Upgraded in Parallel with the Central Controller

In the first example, the production HDS/Distributor AW is upgraded in parallel with the central controller. If necessary, an ICM/IPCC 7.5(1) temporary HDS/Distributor AW is configured prior to central controller upgrade maintenance window to enable real-time reporting and configuration during the time that the production HDS/Distributor AW is off-line being upgraded.

Warning: In order to complete an upgrade successfully, the order of upgrade as defined in this guide MUST be followed.

Table 2: How to perform a TR upgrade where the production HDS/Distributor AW is upgraded in parallel with the Central Controller Upgrade Maintenance Window

Step	Time Estimate	Action	Reference	Comments
1	None.	Upgrade the production system to the required baseline.	Baseline Requirements (page 21)	None.
2	None.	Create the Active Directory environment.	Active Directory and DNS Considerations for Upgrades (page 51)	No impact on the production system.
3	None.	Set up the new hardware.	Setting Up the Hardware (page 35)	No impact on the production system.
4	1 hour	Set up a temporary 7.5(1) HDS/Distributor AW.	Set Up a Temporary ICM/IPCC 7.5(1) AW/HDS (page 126)	Required to enable configuration and real-time reporting while the Side A HDS/Distributor AW is being upgraded.
Start of Central Controller Upgrade Maintenance Window	**********	**********	**********	**********
5	1 hour + data migration time	Upgrade the Side A HDS/Distributor AW.	Distributor AW/HDS Technology Refresh Upgrade (page 119)	Step 6 can begin as soon as the EDMT tool is configured and running. Reporting capacity is diminished until the completion of the Side B Logger, CallRouter and AW/HDS upgrade and side B is brought back into service.

Step	Time Estimate	Action	Reference	Comments
6	1 hour + data migration time	Upgrade the Side A Logger.	Logger Technology Refresh Upgrade: Side A/B (page 133)	Routing is done by the non-upgraded system. Both existing CallRouters are duplexed. The Logger is simplex. Configuration changes are disabled.
7	1 hour	Upgrade the Side A CallRouter.	CallRouter Technology Refresh Upgrade: Side A/B (page 139)	The production system is running simplex on Side B.
8	1 hour per server	Install the WebView server(s) if not collocated on the AW/HDS.	**WebView Installation Guide**[1]	None.
9	1+ hours depending on number of PGs and CIS components	Bring down the production system (CallRouters, Loggers, and AWs). Bring up the new Side A CallRouter and Logger. Point the temporary HDS/Distributor AW, PGs, and CIS components to the new CallRouter & Logger in the new domain.	None.	Default routing occurs from the shutdown of the existing system until the new Side A CallRouter and Logger are brought into service. Real-time reporting is provided via the temporary HDS/Distributor AW set up in step 4. Historical reporting is not available until the Side A AW/HDS upgrade is complete and brought back on line. Reporting capacity remains reduced until the completion of the Side B Logger, CallRouter and AW/HDS upgrade and side B is brought back into service.
10	1 hour	Upgrade the Side B CallRouter.	CallRouter Technology Refresh Upgrade: Side A/B (page 139)	Routing is simplex until the Side B CallRouter is upgraded and brought into service.
11	1 hour + data migration time	Upgrade the Side B Logger.	Logger Technology Refresh Upgrade: Side A/B (page 133)	Configuration is enabled once the Side B Logger is upgraded and brought into service.
End of Central Controller Upgrade Maintenance Window	**********	**********	**********	**********

1) http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/report7/index.htm

Step	Time Estimate	Action	Reference	Comments
12	1 hour + data migration time2-5 hours (1-80 GB)	Upgrade the Side B HDS/Distributor AW.	Distributor AW/HDS Technology Refresh Upgrade (page 119)	This can begin at any point after Step 9.
13	Included in time estimate for Step 5.	Bring up the Upgraded Side A HDS/Distributor AW(s), when available, at any point after Step 8. As soon as the upgraded AW/HDS is brought on line bring down the temporary AW/HDS currently pointing to the A side. If reporting capacity dictates, the temporary AW/HDS could be pointed to the B side until the B side AW/HDS upgrade is complete.	None.	Historical reporting is available once the HDS is brought into service. Real-time reporting is available via the temporary HDS/Distributor AW. Overall reporting capacity is restored via the combination of the Side A and temporary HDS/Distributor AWs.
14	Included in time estimate for Step 12.	Bring up the Upgraded Side B HDS/Distributor AW.	None.	The temporary HDS/Distributor AW can be decommissioned once the Side B HDS/Distributor AW is brought into service. Full reporting functionality and capacity is available at this point.
15	1 hour per node	Upgrade the AWs, PGs, RMS, and CIS components.	Administrative Workstation (AW) Upgrade Procedures (page 115) PG Technology Refresh Upgrade (page 148) Remote Monitoring System (RMS) Upgrade Procedures (page 171) CIS Upgrade Procedures (page 165)	None.

Technology Refresh Example 2: Production HDS/Distributor AW Upgraded Before the Central Controller Upgrade Maintenance Window

In the second example, the production HDS/Distributor AW is upgraded before the central controller upgrade maintenance window. If a secondary HDS/Distributor AW is not available, a Release 7.0(x), 7.1(x), or 7.2(x) temporary HDS/Distributor AW is set up to enable real-time reporting and configuration between the time that the Side A HDS/Distributor AW is upgraded

and the time that the Upgraded HDS/Distributor AW is upgraded and the time the CallRouter, Logger, and Distributor AW are brought into service.

For a technology refresh upgrade of an HDS/Distributor AW, it is only necessary to bring the source HDS off-line during the backup/restore and registry export process.

Note: Instead of configuring and deploying a temporary Release 7.0(x), 7.1(x), or 7.2(x) HDS/Distributor AW, you also have the option of bringing the source HDS back on line. This option is not recommended if maximum reporting capacity and functionality is required during upgrade, since the intent is to upgrade the Side A HDS/Distributor AW well in advance of the Central Controller upgrade maintenance window. If you do choose this option, ensure the Logger purge setting is long enough to prevent data loss.

Warning: In order to complete an upgrade successfully, the order of upgrade as defined in this guide MUST be followed.

Table 3: How to perform a TR upgrade on a system where the production HDS/Distributor AW is upgraded before the Central Controller upgrade maintenance window:

Step	Time Estimate	Action	Reference	Comments
1	None.	Upgrade the production system to the required baseline.	Baseline Requirements (page 21)	None.
2	None.	Create the Active Directory environment.	Active Directory and DNS Considerations for Upgrades (page 51)	No impact on the production system.
3	None.	Set up the new hardware.	Setting Up the Hardware (page 35)	No impact on the production system.
4	1 hour	Set up a temporary Release 7.0(x), 7.1(x), or 7.2(x) HDS/Distributor AW.	Setting Up a Temporary ICM/IPCC AW/HDS (page 126)	Required to enable configuration and real-time reporting until the upgraded CallRouter, Logger, and HDS/Distributor AW are brought into service. If a Side B HDS/Distributor AW is available and the reporting capacity of two HDSs is not required, it is not necessary to set up the temporary HDS/Distributor AW.
5	1 hour + data migration time	Upgrade the Side A HDS/Distributor AW.	Distributor AW/HDS Technology Refresh Upgrade (page 119)	Complete this step before the start of the Central Controller upgrade maintenance window. Reporting is provided by the Side B HDS/Distributor AW and/or the temporary HDS/Distributor AW. In place of the temporary HDS/Distributor AW, it is also possible to bring the un-upgraded

Step	Time Estimate	Action	Reference	Comments
				HDS/Distributor AW back into service after the backup/restore, user domain conversion, and registry export is complete.
6	1 hour per server	Install the WebView server(s) if not co-located on the AW/HDS.	**WebView Installation Guide**[2]	None.
Start of Central Controller Upgrade Maintenance Window	**********	**********	**********	**********
7	1 hour + data migration time	Upgrade the Side A Logger.	Logger Technology Refresh Upgrade: Side A/B (page 133)	Routing is done by the non-upgraded system. Both existing CallRouters are duplexed. The Logger is simplex. Configuration changes are disabled.
8	1 hour	Upgrade the Side A CallRouter.	CallRouter Technology Refresh Upgrade: Side A/B (page 139)	The production system is running simplex on Side B.
9	1+ hours depending on number of PGs and CIS components	Bring down the production system (CallRouters, Loggers, and AWs), bring up the new Side A CallRouter Logger, and HDS/Distributor. Point the PGs and CIS components to the new CallRouter and Logger in the new domain.	None.	Default routing occurs from the shutdown of the existing system until the new Side A CallRouter and Logger are brought into service. Historical and Real-time reporting is provided by the previously upgraded HDS/Distributor AW (step 5). If a temporary Release 7.0(x), 7.1(x), or 7.2(x) HDS/Distributor AW was in use, it can be decommissioned at this point.
10	1 hour	Upgrade the Side B CallRouter.	CallRouter Technology Refresh Upgrade: Side A/B (page 139)	Routing is simplex until the Side B CallRouter is upgraded and brought into service.
11	1 hour + data migration time	Upgrade the Side B Logger.	Logger Technology Refresh Upgrade: Side A/B (page 133)	Configuration is enabled once the Side B Logger is upgraded and brought into service.

2) http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/report7/index.htm

Step	Time Estimate	Action	Reference	Comments
End of Central Controller Upgrade Maintenance Window	**********	**********	**********	**********
12	1 hour + data migration time	Upgrade the Side B HDS/Distributor AW and bring into service once the upgrade is completed.	Distributor AW/HDS Technology Refresh Upgrade (page 119)	This can begin at any point after step 9.
13	1 hour per node	Upgrade the AWs, PGs, RMS, and CIS components	Administrative Workstation (AW) Upgrade Procedures (page 115) PG Technology Refresh Upgrade (page 148) Remote Monitoring System (RMS) Upgrade Procedures (page 171) CIS Upgrade Procedures (page 165)	None.

Common Ground Upgrade Examples

Common Ground Upgrade Example 1: Production HDS/Distributor AW Upgraded in Parallel with Central Controller

Two Common Ground upgrade examples are provided below. Both examples assume redundant configurations with Side A and Side B CallRouters and Loggers, and that Side A and Side B HDS/Distributor AWs are part of the system being upgraded and are required to support the number of reporting users. The examples therefore include the deployment of a temporary HDS/Distributor AW to maintain maximum system functionality and reporting capacity during the upgrade process.

Warning: In order to complete an upgrade successfully, the order of upgrade as defined in this guide MUST be followed.

The deployment of a temporary HDS/Distributor AW may not be necessary depending on:

- the contact center hours of operation
- the estimated upgrade time for each ICM/IPCC node
- whether one or two HDS/Distributor AWs are deployed

- the reporting user capacity required during upgrade
- other operational factors

The temporary HDS/Distributor AW does not provide historical reporting, only real-time reporting is provided. Both examples assume Side A is upgraded first, although the B side can be upgraded first.

In the first example, the production HDS/Distributor AW is upgraded in parallel with the Central Controller. If necessary, a Release 7.5(1) temporary HDS/Distributor AW is configured prior to the Central Controller upgrade maintenance window to enable real-time reporting and configuration during the time that the production HDS/Distributor AW is off-line being upgraded.

Table 4: How to perform a CG upgrade where the production HDS/Distributor AW is upgraded in parallel with the Central Controller Upgrade Maintenance Window:

Step	Time Estimate	Action	Reference	Comments
1	None.	Upgrade the production system to the required baseline.	Baseline Requirements (page 21)	None.
2	None.	Create the Active Directory environment.	Active Directory and DNS Considerations for Upgrades (page 51)	No impact on the production system.
3	1 hour	Set up a temporary 7.5(1) HDS/Distributor AW.	Setting Up a Temporary ICM/IPCC AW/HDS (page 126)	Required to enable configuration and real-time reporting while the Side A HDS/Distributor AW is being upgraded.
Start of Central Controller Upgrade Maintenance Window	**********	**********	**********	**********
4	1 hour + data migration time	Upgrade the Side A HDS/Distributor AW.	Distributor AW/HDS Common Ground Upgrade (page 125)	Step 5 can begin as soon as the EDMT is configured and running. Reporting is provided by the Side B HDS/Distributor AW, although reporting capacity is diminished until the completion of both sides of the Central Controller have been upgraded and brought back on-line.
5	1 hour + data migration time	Upgrade the Side A Logger.	Logger Common Ground Upgrade: Side A/B (page 135)	Routing done by non-upgraded system. Both existing CallRouters are duplexed. The Logger is simplex.

Step	Time Estimate	Action	Reference	Comments
				Configuration changes are disabled.
6	1 hour	Upgrade the Side A CallRouter.	CallRouter Common Ground Upgrade: Side A (page 140)	The production system is running simplex on Side B.
7	1 hour per server	Install the WebView server(s) if not co-located on the AW/HDS.	**WebView Installation Guide**[3]	None.
8	1+ hours	Bring down the side B CallRouter, Logger, and all distributor and Client AWs. Bring up the upgraded Side A CallRouter and Logger. Point the temporary HDS/Distributor AW to the upgraded Side A CallRouter and Logger.	None. How to Bring Side A into Service (page 141) None.	Default routing occurs from the shutdown of the Side B CallRouter until the upgraded Side A CallRouter and Logger are brought into service. Real-time reporting is provided via the temporary HDS/Distributor AW set up in step 3. Reporting capacity is diminished until the Side A HDS/Distributor AW is brought into service.
9	1 hour	Upgrade the Side B CallRouter.	CallRouter Common Ground Upgrade: Side B (page 143)	Routing is simplex until the Side B CallRouter is upgraded and brought into service.
10	1 hour + data migration time	Upgrade the Side B Logger.	Logger Common Ground Upgrade: Side A/B (page 135)	Configuration is enabled once the Side B Logger is upgraded and brought into service.
End of Central Controller Upgrade Maintenance Window	**********	**********	**********	**********
11	1 hour + data migration time	Upgrade the Side B HDS/Distributor AW.	Distributor AW/HDS Common Ground Upgrade (page 125)	This can begin at any point after step 8.
12	Included in time estimate for Step 4.	Bring down the temporary AW/HDS and then bring up the upgraded AW/HDS (or vice versa) when available, at any point after Step 8.	None.	Historical and Realtime reporting is available via the upgraded AW/HDS once the upgraded AW/HDS is brought on line. Reporting capacity is still diminished until the completion of the upgrade of the B side AW/HDS and it is brought back on-line.

3) http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/report7/index.htm

Step	Time Estimate	Action	Reference	Comments
13	Included in time estimate for Step 12.	Bring up the Upgraded Side B HDS/Distributor AW.	None.	The temporary HDS/Distributor AW can be decommissioned once the Side B HDS/Distributor AW is brought into service. Full reporting functionality and capacity is available at this point.
14	1 hour per node	Upgrade the AWs, PGs, RMS, and CIS components.	Administrative Workstation (AW) Upgrade Procedures (page 115) Peripheral Gateway (PG) Upgrade Procedures (page 147) Remote Monitoring System (RMS) Upgrade Procedures (page 171) CIS Upgrade Procedures (page 165)	None.

Common Ground Upgrade Example 2: Production HDS/Distributor AW Upgraded Before the Central Controller Upgrade Maintenance Window

In the second example, the production HDS/Distributor AW is upgraded before the Central Controller upgrade maintenance window. If a secondary HDS/Distributor AW is not available, a Release 7.0(x), 7.1(x), or 7.2(x) temporary HDS/Distributor AW is set up to enable real-time reporting and configuration between the time that the Side A HDS/Distributor AW is upgraded and the upgraded CallRouter, Logger, and Distributor AW are brought into service. Do not use this option if maximum reporting capacity and functionality is required during upgrade, since the intent is to upgrade the Side A HDS/Distributor AW well in advance of the Central Controller upgrade maintenance window.

Warning: In order to complete an upgrade successfully, the order of upgrade as defined in this guide MUST be followed.

Table 5: How to perform a CG upgrade on a system where the production HDS/Distributor AW is upgraded before the Central Controller upgrade maintenance window:

Step	Time Estimate	Action	Reference	Comments
1	None.	Upgrade the production system to the required baseline.	Baseline Requirements (page 21)	None.
2	None.	Create the Active Directory environment.	Active Directory and DNS Considerations for Upgrades (page 51)	No impact on the production system.

Step	Time Estimate	Action	Reference	Comments
3	1 hour	Set up temporary Release 7.0(x), 7.1(x), or 7.2(x) HDS/Distributor AW.	Setting Up a Temporary ICM/IPCC AW/HDS (page 126)	Required to enable configuration and real-time reporting until the upgraded CallRouter, Logger, and HDS/Distributor AW are brought into service. If a Side B HDS/Distributor AW is available and the reporting capacity of two HDSs is not required, it is not necessary to set up the temporary HDS/Distributor AW.
4	1 hour + data migration time	Upgrade the Side A HDS/Distributor AW.	Distributor AW/HDS Common Ground Upgrade (page 125)	Complete this step before the start of the Central Controller upgrade maintenance window. Reporting is provided by the Side B HDS/Distributor AW and/or the temporary HDS/Distributor AW. If only a temporary AW/HDS is available historical reporting will not be available until after the completion of the A side upgrade.
5	1 hour per server	Install the WebView server(s) if not co-located on the AW/HDS.	**WebView Installation Guide**[4]	None.
Start of Central Controller Upgrade Maintenance Window	**********	**********	**********	**********
6	1 hour + data migration time	Upgrade the Side A Logger.	Logger Common Ground Upgrade: Side A/B (page 135)	Routing is done by the non-upgraded duplexed CallRouters. The Logger is simplex. Configuration changes are disabled.
7	1 hour	Upgrade the Side A CallRouter.	CallRouter Common Ground Upgrade: Side A (page 140)	The production system is running simplex on Side B.

4) http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/report7/index.htm

Step	Time Estimate	Action	Reference	Comments
8	1+ hours depending on number of PGs and CIS components	Bring down the side B CallRouter, Logger, and all distributor and client AWs. Bring up the upgraded Side A CallRouter, Logger, and HDS/Distributor AW.	None. How to Bring Side A into Service (page 141)	Default routing occurs from the shutdown of the Side B CallRouter until the upgraded Side A CallRouter and Logger are brought into service. Reporting is provided by the previously upgraded Side A HDS/Distributor AW. If a temporary Release 7.0(x), 7.1(x), or 7.2(x) HDS/Distributor AW was in use, it can be decommissioned at this point.
9	1 hour	Upgrade the Side B Logger.	Logger Common Ground Upgrade: Side A/B (page 135)	Routing is done by the upgraded CallRouter and Logger - simplex.
10	1 hour + data migration time	Upgrade Side B CallRouter.	CallRouter Common Ground Upgrade: Side B (page 143)	Configuration is enabled once the Side B Logger is upgraded and brought into service.
End of Central Controller Upgrade Maintenance Window	**********	**********	**********	**********
11	1 hour + data migration time	Upgrade the Side B HDS/Distributor AW and bring it into service once the upgrade is completed.	Distributor AW/HDS Common Ground Upgrade (page 125)	This can begin at any point after step 8.
12	1 hour per node	Upgrade the AWs, PGs, RMS, and CIS components.	Administrative Workstation (AW) Upgrade Procedures (page 115) Peripheral Gateway (PG) Upgrade Procedures (page 147) Remote Monitoring System (RMS) Upgrade Procedures (page 171) CIS Upgrade Procedures (page 165)	None.

ICM/IPCC Component Upgrade Process

Following chapters provide information on the upgrade process for each major ICM/IPCC component. The process assumes that most components are configured redundantly, typically Side A and Side B. For ICM/IPCC 7.5(1), the database migration uses a process and tool called the Enhanced Database Migration Tool (EDMT) (see Enhanced Database Migration Tool for ICM/IPCC 7.5(1) (page 59)). This tool is referenced in the step-by-step procedures in this document.

Note:

- The phrase “ICM/IPCC core components” or “core components” refers to the following ICM components: CallRouter, Logger, Administrator Workstations (AWs), Peripheral Gateways (PGs), CTI Servers (CGs), CTI OS Servers, Historical Data Server (HDS), WebView Server.
- The phrase “ICM Central Controller” or “ICM Central Controller components” refers to the following ICM components: CallRouter, Logger, key Distributor AW (with or without HDS, HDS with or without WebView Server).

Chapter 10

Administrative Workstation (AW) Upgrade Procedures

Introduction

There are four different types of Administrator Workstations (AWs) supported in ICM/IPCC Release 7.5(1) deployments:

- Distributor AW with HDS and WebView Server (primary and secondary)
- Distributor AW with HDS without WebView Server (WebView Servers on dedicated hardware)
- Distributor AW without HDS
- Client AW

In previous releases, WebView Servers were sometimes deployed on non-HDS Distributor AWs. If this is the case, the WebView servers must be moved either onto AW/HDS, or on separate servers.

The procedures for Distributor AW/HDSs, Non-HDS Distributor AWs, Client AWs, and creating a temporary AW/HDS are presented in the following sections.

Note:

- It is only necessary to run the Domain Manager on the first component to be upgraded (Distributor AW/HDS or Logger) to Release 7.5(1) when adding that instance to the appropriate Active Directory Instance organizational unit.
- Creating a temporary AW/HDS is required when real time reporting must remain available during the upgrade of a system having a single HDS/WebView Server.

Collocation of WebView server on a non-HDS AW is not supported for Release 7.5(1). If WebView is installed in on the non-HDS Distributor AW of the system being upgraded, the components which make up WebView (Infomaker, ServletExec, EA Server, etc.) must be uninstalled before beginning the upgrade.

Prior to creating an ICM 7.5(1) database, look up and record the size of your existing ICM database.

AW/HDS/WebView Server Pre-upgrade Preparation

Pre-upgrade preparation is an integral part of the upgrade process. Perform the following on all AW, HDS, and/or WebView servers to assist in recovery in the event of a catastrophic upgrade failure:

Step 1 Perform a full SQL backup of the AW DB using the Microsoft SQL Backup and Restore utility.

Step 2 Perform a full SQL backup of the ICM HDS DB using the Microsoft SQL Backup and Restore utility.

Note: For ICM/IPCC 7.0(0) and later systems, there is a restriction on the number of HDSs that can be configured on each Logger side, as well as the number of WebView servers that can be configured for each HDS. Ensure there are no more than two (2) HDSs per Logger side, with no more than four (4) WebView servers configured for each HDS. Refer to How to reduce the number of HDSs (page 116) for additional information.

Step 3 Perform a full SQL backup of the WebView DB using the Microsoft SQL Backup and Restore utility.

Step 4 Record the current size of the log files.

Step 5 Copy the Cisco registry key.

Step 6 Copy the ICM/bin directory.

Step 7 Copy the *c:\winnt\awref.ini* file.

How to reduce the number of HDSs

The following is for use on ICM/IPCC Release 7.0(0), and later, systems to reduce the number of HDSs per Logger side to two (2) ,with up to four (4) WebView Servers configured for each HDS.

The example following the steps illustrates this procedure.

Step 1 Select two (2) HDSs to keep per Logger side.

Step 2 Detach/remove all other HDSs from each Logger side.

Step 3 Remove the WebView server(s) from the remaining HDS(s).

Step 4 Install the equivalent number of WebView servers as those removed.

Step 5 Configure the WebView servers to point to the appropriate HDS on each Logger side (with a limit of four servers maximum configured to a single HDS).

Example:

Figure 21: Original Configuration

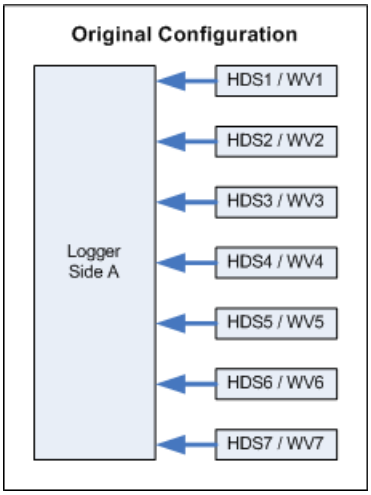


Figure 22: Select HDSs to Keep

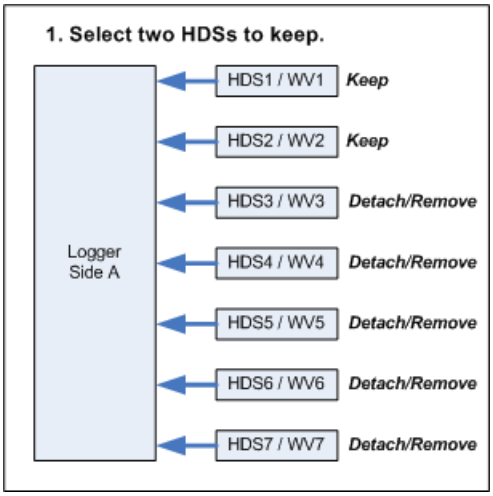


Figure 23: Detach Remaining HDSs

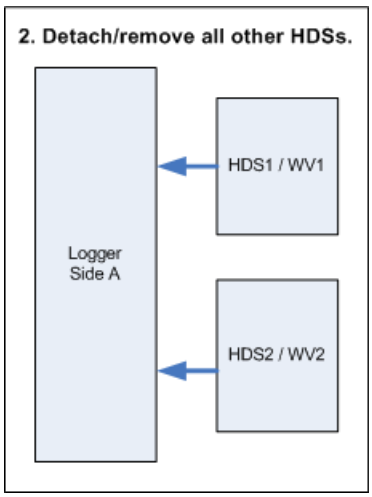


Figure 24: Remove WebView Servers

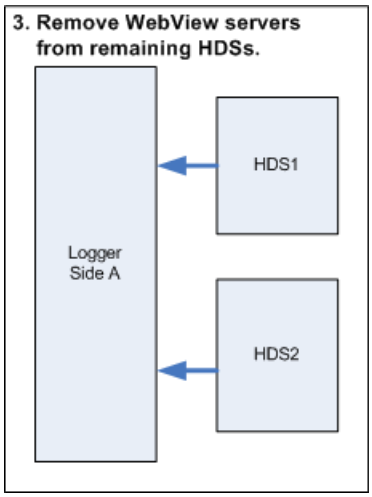
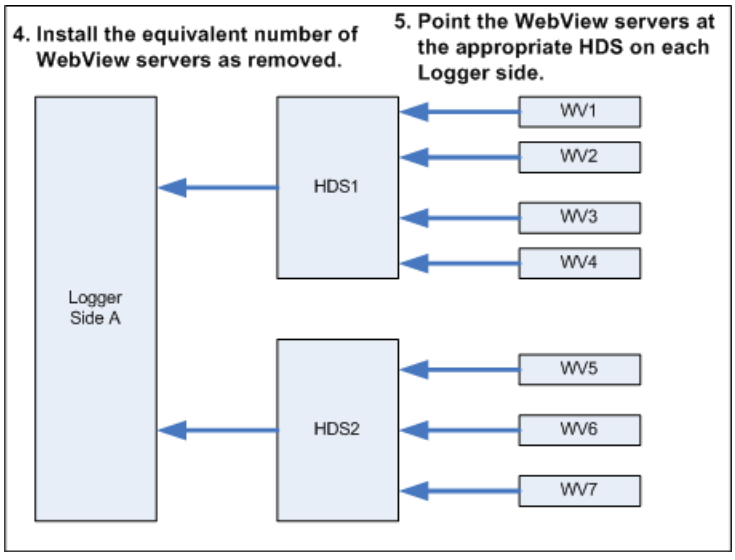


Figure 25: Install and Point WebView Servers



Distributor AW/HDS Technology Refresh Upgrade

Upgrading the Primary/Secondary AW/HDS

Note:

- If WebView Server is to be collocated on the same server as the AW/HDS start at Step 1.
- If WebView Server is not to be collocated on the same server as the AW/HDS, start at Step 8.

Install IIS on the new AW/HDS. IIS is usually installed as part of the installation of Windows 2003. However, you can install IIS after installing Windows 2003. IIS must be installed IIS to support WebView Browser functionality. You need to consider which server needs this component. If you are going to install WebView on the AW/HDS then you must install IIS on the AW/HDS. If you are going to install WebView on a separate server then you must install IIS on that server instead.

Note:

- **Important:** The Windows Firewall configuration scripts must be deployed before this server can accept network connections. This must been done as part of the staging tasks.
- When installing IIS you will need files from the Windows 2003 CD.

Step 1 Install IIS after installing Windows 2003.

a. Click **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.

b. Select **Configure Windows**, click **Components**, and then follow the on-screen instructions to install, remove, or add components to IIS.

c. Use the ICM/IPCC 7.5(1) Third Party Tools CD to install JDK, ServletExec, and EA Server.

d. Print and read the *Read Me* file on the WebView 3rd Party Installer CD 7.5(1).

This file describes the software and provides installation instructions. Various settings described in the *Read Me* file appear on certain setup screens.

Step 2 Install the WebView Third Party software.

a. Ensure that IIS is installed and is accessible on the system where WebView is being installed. Third-party install fails if IIS is not installed.

b. Run **setup.exe** from the ICM Third Party Installer CD 7.5(1).

c. Reboot the server when setup completes.

d. Set the following to make sure that the cache is updated at each new view of a real-time report:

- In the Internet Explorer window, select **Tools** > **Internet Options**.
- Select the **General** tab.
- On the General Settings tab page, in the Temporary Internet Files sections, click **Settings**.

e. In the Settings dialog box, enable the **Every Visit to the Page** option, then click **OK**.

f. Click **OK** in the **Internet Options** dialog box.

Note: WebView users are configured through the ICM Configuration Manager and passwords default to a given expiration time frame set by the user's domain. If a WebView user's password expires, the user cannot reset the password by WebView access, but would have to request that the ICM System Administrator set a new password. Once the user is created, the ICM System Administrator has the option to set WebView User passwords to never expire through Active Directory Users and Computers.

Step 3 Create a backup of the WebView database (wvdb) on the production AW/HDS using the Microsoft SQL Backup and Restore utility.

Step 4 Save any WebView public and/or private reports or favorites that exist on the production AW/HDS, then copy them to the new AW/HDS. Move custom templates and saved reports during a TR upgrade.

a. Before running ICM setup, create the folder path: **`\icm\<instance>\`**

b. For **custom templates**\aw\custom directory from the old machine to the new machine.

Step 5 Create the wvdb on the new AW/HDS using SQL Enterprise Manager .

When migrating from an older ICM/IPCC release to a newer ICM/IPCC release, you need to lookup the database size of the existing ICM database. This number is used later in the process to create an ICM database of the same size. This value may be increased depending on planned ICM usage patterns. To find the database size refer to How to Determine the Size of an ICM Database (page 174).

The size and configuration of the tempdb database during data migration differs for the parameters used in a production system. Set the tempdb size for each case (see How to set the tempdb database size (page 175)).

Step 6 Restore the backup version of wvdb on the new AW/HDS using the Microsoft SQL Backup and Restore utility.

Step 7 Prepare to move scheduled report jobs to the new WebView server:

a. Ensure the existing WebView server machine is on.

b. Ensure the new WebView server machine on.

c. Create a Windows account that has “Administrator” privileges on both the existing and the new WebView server machines.

d. Confirm that "Task Scheduler" service is running on both machines by selecting **Control Panel** > **Administrative Tools** > **Services**.

Step 8 Move scheduled report jobs to the new WebView Server.

a. Login to the existing WebView server machine using an account that has "Administrator" privilege on both the existing and the new WebView server machines.

b. Select **Control Panel** > **Scheduled tasks** to open Scheduled Tasks.

c. From the available tasks, copy tasks related to WebView scheduled jobs.

Note: WebView scheduled jobs can be identified by checking the "Run" command of each job. WebView scheduled jobs have "scheduler.exe" in their run command. To check the "Run" command of each job, select a job and open its properties.

d. Select and copy the jobs that need to be moved to new WebView machine.

e. Open Windows explorer and enter **`\\<New WebView machine name>`**. If prompted, enter the login name and password of an account that has "Administrator" privileges on the new machine.

f. In the explorer window, find the "Scheduled Tasks" item. Double-click and open **Scheduled Tasks** on the target machine.

g. Paste the tasks copied from existing WebView server to new WebView server.

h. Verify that all WebView tasks are copied successfully.

i. WebView scheduled jobs start printing and/or saving reports on the new machine once:

- WebView is available on new machine
- WebView database has been restored from old WebView server to new WebView server

Step 9 Use the ICM/IPCC data migration tool (EDMT) to migrate the HDS database from the production AW/HDS to the new AW/HDS.

Note: Prior to installing the EDMT, prerequisites must be completed.

In the case of a Technology Refresh upgrade, EDMT must be installed and configured on the new BOM (refer to the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)) compliant destination database server machine.

Refer to the indicated sections of this document, or the "How to ..." section of the EDMT online help, for the details of each of the following tasks:

a. Perform the EDMT installation prerequisites (see *How to perform the EDMT installation prerequisites*).

b. Install the EDMT (see How to install the EDMT (page 60)).

c. Run the EDMT (see How to run the EDMT (page 60)).

d. Perform the EDMT Technology Refresh Migration - Side A (see Technology Refresh Migration Sequence (page 66)).

- Select the Migration Type (see *How to select the Migration Type*).
- Click **Next** to continue to the Source and Destination Database Connection panels. Enter the information required to connect to the migration source database server (see *How to enter the information required to connect to the migration source database server*).
  - Host Name/IP Address
  - ICM Database Name
  - SQL Server Port Number
- Select Authentication Type:
  - Windows Authentication (normally used)
  - SQL Server Authentication

  The following fields are not requested for Windows Authentication:
  - Windows Domain Name
  - Windows Username
  - Windows Password

e. Continue to the migration Destination Database Connection panel (see *How to enter the information required to connect to the migration destination database server*).

Enter the information required to connect to the migration destination database server:

- Host Name/IP Address
- ICM Database Name
- SQL Server Port Number
- Select Authentication Type:
  - Windows Authentication (normally used)
  - SQL Server Authentication

  The following fields are not requested for Windows Authentication:

– Windows Domain Name

– Windows Username

– Windows Password

f. Click **Next** to continue to the Backup Connection and Restore Location panels. Enter the information required for EDMT to backup the migration source database (see *How to enter the information required for EDMT to backup the migration source database*).

- Host Name/IP Address
- Windows Share Name
- Windows Share Username
- Windows Share Password

g. Continue to the Restore Location panel and enter the restore location for the data file and the log file (see *How to enter the restore location for the data file and the log file*).

- Data File Location
- Log File Location

h. Click **Next** to continue to the Migration Control panel. Click **Start Migration**to begin the data migration process. The following warning appears:

Data and schema corruption may result if this process is interrupted. The ICM/IPCC database would then be in an inconsistent state and need to be restored from backup. Are you sure you want to start the data migration?

Click **Yes** to start the data migration.

Click **No** to abort the data migration.

Select the appropriate choice.

Step 10 Export the ICM AW/HDS registry from the production AW/HDS, and import the registry to the new AW/HDS.

Note: Refer to Exporting and Importing the Registry (page 125) for additional information.

Step 11 Import the saved ICM AW/HDS registry.

Note:

- Importing a registry file replaces portions of the registry. Do not import a registry file on the existing production system. You can import the Cisco Systems, Inc. registry into the new Windows 2003 system.
- Refer to Exporting and Importing the Registry (page 125) for additional information.

Step 12 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD on the new AW/HDS. Apply the automated hardening when prompted.

Step 13 Using Domain Manager, add the AW/HDS instance to the appropriate Active Directory Instance organizational unit.

Note: This step only needs to be run if it is the first component to be upgraded to Release 7.5(1).

Step 14 From ICM setup, edit the instance by inserting the new domain name (select the OU created in the previous step).

Step 15 From ICM setup, edit the AW component and make the necessary changes based on the environment in which the new AW/HDS is to run.

Step 16 Edit the WebView component and make the necessary changes based on the environment in which the new AW/HDS is to run.

Note:

- If WebView was previously installed, the WebView component is also visible from ICM setup.
- If WebView was not previously installed but is desired, install the WebView Third Party software first, then add the WebView component. Enter the appropriate configuration data when prompted.

Step 17 Using ICM Service Control, set all ICM processes on the new AW/HDS to **Manual Start**.

Step 18 Exit and then rerun setup.

Step 19 When the main setup screen appears, select **Upgrade All**.

Step 20 Reboot the AW/HDS.

Step 21 Run **`wvusersync.bat /update`** (located in the \ICM\web\webview\wvdb directory) on the WebView server.

Step 22 Install the latest 7.5 Maintenance Release and any required Engineering Specials on the new AW/HDS.

Step 23 If required, re-execute the process to private label WebView.

Step 24 If the Outbound Option is in use and the Campaign Manager has been upgraded, open the Campaign Manager configuration tool.

a. On the **Call Target** tab, configure the correct daylight savings time option for each campaign.

b. On the **Skill Group Selection** tab, add a dialed number in the **Dialed Number** field for each skill group selection entry in every campaign.

Step 25 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the new AW/HDS.

Step 26 Start the upgraded Primary AW/HDS anytime after the previous step is completed and the Side A Central Controller has been upgraded to and is running.

Exporting and Importing the Registry

Step 1 **How to export a registry file**

a. Open a command prompt and type **`regedit`** or select **Start** > **Run**, enter **`regedit`**. then click **OK**.

b. Select **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.**.

c. Click **Registry** > **Export registry file**.

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

e. Enter a filename to be remembered.

f. Click **Save**.

Step 2 **How to import a registry file**

a. Open a command prompt and type **`regedit`** or select **Start** > **Run**, enter **`regedit`**. then click **OK**.

b. Select HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.

c. Click **Registry** > **Import registry file**.

d. Browse the directory to where the saved registry file is stored, then click **Open**.

e. Verify that the contents has been imported by looking at the entries under HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.

f. Click **Registry** > **Exit**.

Distributor AW/HDS Common Ground Upgrade

Step 1 If not already done, using ICM Service Control, stop all ICM services on the AW/HDS.

Step 2 Using ICM Service Control, change all ICM services on the AW/HDS to Manual Restart.

Step 3 Using third party imaging or “ghost” software, perform a full system backup of the AW/HDS so that it can be restored if a critical failure occurs during the common ground upgrade process.

Step 4 Uninstall the Cisco Security Agent 4.0 Agent and the ICM Policy.

Note: If you plan to change domains, do so at this point.

Step 5 Upgrade Third Party software such as virus protection software, VNC, and PC Anywhere.

Step 6 Reboot the AW/HDS.

Step 7 Install the Release 2.3(1) Support Tools agent.

Note: It is not necessary to uninstall older versions of the Support Tools agent.

Step 8 If WebView Server is collocated on the same server as the AW/HDS:

a. Remove Infomaker if it was previously installed.

Note: In 7.5(1), Infomaker must be installed on a separate, non-ICM machine.

b. Remove any pre-existing versions of EAServer (Jaguar).

c. Use the ICM 7.5(1) Third Party Tools CD to upgrade the JDK, ServletExec, and EA Server.

Step 9 Use the EDMT to update the HDS database to Release 7.5(1) (see Common Ground EDMT Wizard Sequence (page 63)).

Step 10 Using the Domain Manager, add the AW/HDS instance to the appropriate Active Directory Instance organizational unit.

Note: This step only needs to be run if it is the first component to be upgraded to Release 7.5(1).

Step 11 While in ICM setup, edit the AW and HDS components and review all entries.

Step 12 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD on the AW/HDS. When the main setup screen appears, click **Upgrade All**.

Step 13 If the Active Directory domain is changing as part of the upgrade, run ICM setup.exe from the ICM/bin directory, edit the instance and insert the new domain name.

Step 14 Reboot the AW/HDS.

Step 15 Install the latest 7.5 Maintenance Release and any required Engineering Specials on the AW/HDS

Step 16 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the new AW/HDS.

Setting Up a Temporary ICM/IPCC AW/HDS

Based on the upgrade you are performing, you can create a temporary ICM/IPCC AW/HDS to provide reporting during the upgrade process. You may need to create a temporary AW/HDS

for either the existing ICM/IPCC 7.0(x), 7.1(x), or 7.2(x) system or for the new ICM/IPCC 7.5(1) system. The maintenance windows discussed below correspond to those in the Figure 1: Upgrading a Complex, Multi-media, ICM/IPCC System (page 26).

Setting Up a Temporary ICM/IPCC AW/HDS for an ICM/IPCC 7.0(x), 7.1(x), or 7.2(x) System

Create a temporary ICM/IPCC 7.0(x), 7.1(x), or 7.2(x) AW/HDS if you are starting with only a Primary AW/HDS to provide reporting. During the first maintenance window, while you upgrade side A and the Primary AW/HDS, the temporary AW/HDS provides real time and historical reporting, getting data from side B.

In the second maintenance window, side A is now upgraded and coming up, side B is down being upgraded, and no ICM/IPCC 7.5(1) AW is available. This results in no reporting capabilities in the second maintenance window until the Primary AW/HD is upgraded and back up.

Step 1 Run ICM setup on either a new machine or an existing machine that will not be upgraded during the first maintenance window.

Step 2 Using ICM setup, create an AW/HDS component on the existing ICM/IPCC 7.0(x), 7.1(x), or 7.2(x) system.

Step 3 Upgrade the rest of the existing system using the appropriate procedure from the *Upgrade Procedures* section of this guide.

Setting Up a Temporary ICM/IPCC AW/HDS for an ICM/IPCC 7.5(1) System

Create a temporary ICM/IPCC 7.5(1) AW/HDS if you are starting with both a Primary and a Secondary AW/HDS to provide reporting. During the first maintenance window, while you upgrade side A and the Primary AW/HDS, the Secondary AW/HDS provides real time and historical reporting, getting data from side B.

In the second maintenance window, the upgraded side A is coming up, side B is down being upgraded. The temporary ICM/IPCC 7.5(1) AW/HDS provides real time reporting only, getting data from the upgraded side A. Normal reporting (real time and historical) is restored when the Primary AW/HDS is upgraded to ICM/IPCC 7.5(1) and is up and running.

Step 1 Run ICM setup on new BOM compliant hardware.

Step 2 Perform a fresh installation of an ICM/IPCC 7.5(1) AW/HDS.

Step 3 Point the new ICM/IPCC 7.5(1) AW/HDS to the ICM/IPCC 7.5(1) Logger and CallRouter.

Step 4 Upgrade the Logger to ICM/IPCC 7.5(1).

Step 5 Upgrade the CallRouter to ICM/IPCC 7.5(1).

Step 6 Bring up the ICM/IPCC 7.5(1) Logger and CallRouter.

Step 7 Bring down all the other ICM/IPCC 7.5(1) components.

Step 8 Bring up the new ICM/IPCC 7.5(1) AW/HDS

Step 9 Upgrade the rest of the existing system using the appropriate procedure from the *Upgrade Procedures* section of this guide.

Non-HDS Distributor AW Technology Refresh Upgrades

Step 1 If not already done, stop the ICM services on the production distributor AW using the ICM Service Control.

Step 2 Export the ICM AW registry from the production AW, and import the registry to the new AW.

Note: Refer to Exporting and Importing the Registry (page 125) for additional information.

Step 3 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD on the new AW. Apply the automated hardening when prompted.

Step 4 From ICM setup, edit the instance and insert the new domain name.

Step 5 From ICM setup, edit the AW component and make the necessary changes based on the environment in which the new Logger is to be run. For ICM/IPCC 7.5(1), make sure WebView is not checked since WebView Server is not supported on a non-HDS distributor AW.

Step 6 Using ICM Service Control, set all ICM processes on the new AW to **Manual Start**.

Step 7 Exit and then rerun setup. When the main setup screen appears, select **Upgrade All**.

Step 8 Reboot the AW.

Step 9 Install the latest ICM/IPCC 7.5 Maintenance Release and any required Engineering Specials on the new AW.

Step 10 If the Outbound Option is in use and the Campaign Manager has been upgraded, open the Campaign Manager configuration tool.

a. On the **Call Target** tab to configure the correct daylight savings time option for each campaign.

b. On the **Skill Group Selection** tab, add a dialed number in the **Dialed Number** field for each skill group selection entry in every campaign.

Step 11 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the new AW.

Non-HDS Distributor AW Common Ground Upgrades

Step 1 If not already done, using ICM Service Control, stop all ICM services on the AW

Step 2 Using ICM Service Control, change all ICM services on the AW to **Manual Restart**.

Step 3 Using third party imaging or "ghost" software, perform a full system backup of the AW server so that it can be restored if a critical failure occurs during the common ground upgrade process.

Step 4 Uninstall the Cisco Security Agent 4.0 Agent and the ICM Policy.

Note: If you plan to change domains, do so at this point.

Step 5 Upgrade Third Party software such as virus protection software, VNC, or PCAnywhere.

Step 6 Reboot the AW.

Step 7 Install the Release 2.3(1) Support Tools agent. It is not necessary to uninstall older versions of the Support Tools agent.

Step 8 Using the Domain Manager, add the AW instance to the appropriate Active Directory Instance Organizational Unit.

Step 9 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD and select **Upgrade All** on the main setup screen to upgrade all ICM components on the AW.

Step 10 If the Active Directory domain is changing as part of the upgrade, run ICM setup.exe from the ICM/bin directory, edit the instance and insert the new domain name on the AW.

Step 11 While in ICM setup, edit the AW component and review all entries.

Step 12 Reboot the AW.

Step 13 Install the latest 7.5 Maintenance Release and any required Engineering Specials on the updated CallRouter.

Step 14 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the upgraded CallRouter.

Client AW Technology Refresh Upgrades

Step 1 Set up the new server as outlined in Set up the New Hardware.

Step 2 Using the ICM Service Control, stop all ICM services on the production AW being replaced.

Step 3 Export the ICM registry from production Client AW, and import the registry to the new Client AW.

Note: Refer to Exporting and Importing the Registry (page 125) for additional information.

Step 4 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD on the new AW.

Step 5 From ICM setup, edit all instances on the new server and insert the new domain name.

Step 6 From ICM setup, edit all ICM components on the new server and make the necessary changes based on the environment in which the new AW is to run.

Step 7 Exit and then rerun setup. When the main setup screen appears, select **Upgrade All**.

Step 8 Using ICM Service Control, set the ICM processes on the new AW to **Manual Start**.

Step 9 Reboot the new AW .

Step 10 Install the latest ICM/IPCC 7.5 Maintenance Release and any required Engineering Specials on the new AW.

Step 11 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the new AW.

Step 12 Using ICM Service Control, start the ICM processes on the new AW.

Step 13 Using ICM Service Control, set the ICM processes on the new AW to **Automatic Start**.

Client AW Common Ground Upgrade

Step 1 Using ICM Service Control, stop all ICM services on the AW.

Step 2 Using ICM Service Control, change all ICM services on the AW to **Manual Restart**.

Step 3 Using third party imaging or “ghost” software, perform a full system backup of the AW server so that it can be restored if a critical failure occurs during the common ground upgrade process.

Step 4 Uninstall the Cisco Security Agent 4.0 Agent and the ICM Policy.

Note: If you plan to change domains, do so at this point.

Step 5 Upgrade Third Party software such as virus protection software, VNC, or PCAnywhere.

Step 6 Reboot the AW.

Step 7 Install the Release 2.3(1) Support Tools agent. It is not necessary to uninstall older versions of the Support Tools agent.

Step 8 Using the Domain Manager, add the AW instance to the appropriate Active Directory Instance Organizational Unit.

Step 9 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD and select **Upgrade All** on the main setup screen to upgrade all ICM components on the AW.

Step 10 If the Active Directory domain is changing as part of the upgrade, run ICM setup.exe from the ICM/bin directory, edit the instance and insert the new domain name on the AW.

Step 11 While in ICM setup, edit the AW component and review all entries.

Step 12 Reboot the AW.

Step 13 Install the latest 7.5 Maintenance Release and any required Engineering Specials on the AW.

Step 14 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the AW.

Upgrading WebView Server(s) Not Collocated on the AW/HDS

When upgrading a WebView Server that is not collated on the AW/HDS, perform the following:

Step 1 Back up all Saved and Custom reports if applicable.

Step 2 Run the 7.5(1) installer and select **Upgrade All**. In addition to upgrading to Release 7.5(1), this also upgrades JDK.

Step 3 Restart the machine after installation.

For additional information refer to the **WebView Installation and Administration Guide Cisco ICM/IPCC Enterprise & Hosted, Release 7.0(0)** (http://www.cisco.com/en/US/products/sw/custcosw/ps4145/prod_installation_guides_list.html).

Note: Important: The Windows Firewall configuration scripts must be deployed before this server can accept network connections. This is done as part of the staging tasks.

Chapter 11

Logger Upgrade Procedures

Logger Pre-upgrade Preparation

Pre-upgrade preparation is an integral part of the upgrade process.

Preparing the Logger for recovery in the event of a catastrophic upgrade failure

Perform the following on the Logger:

Step 1 Perform a full SQL backup of the ICM DB using the Microsoft SQL Backup and Restore utility.

Step 2 Perform a full SQL backup of the Outbound DB using the Microsoft SQL Backup and Restore utility, if applicable.

Step 3 Record the current size of the log files.

Step 4 Copy the Cisco registry key (Cisco Systems, Inc.).

Step 5 Copy the ICM/bin directory.

Logger Technology Refresh Upgrade: Side A/B

The following procedure is used to perform a Technology Refresh upgrade on both sides of the Logger. When upgrading Side A use the procedure as is. When upgrading Side B, simply replace “Side A” with “Side B” in the procedure.

Note: Important: The Windows Firewall configuration scripts must be deployed before this server can accept network connections. This is done as part of the staging tasks.

How to perform a TR upgrade on the Logger

1. Disable configuration changes.
   - Set the HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\ICM\<instancename>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance key to 1 on both sides of the CallRouter in the system being upgraded.

     Note: RouterA in the registry key above is RouterB on the Side B CallRouter.
   - Verify that configuration changes are prevented. The following message is displayed when attempting to save a configuration change:

     Failed to update the database. Exclusive access to the CallRouter denied because configuration changes are currently disabled in the router registry.
2. Using the ICM Service Control, stop the ICM services on the Side A production Logger, Distributor AW, and HDS.
3. If the Outbound Option is in use, back up the Outbound Option private database using the SQL Server Enterprise Manager. The campaign manager is present on only one of the redundant Loggers, and needs to be upgraded on only that Logger.

   Note:
   - Dialers and their associated PG must be upgraded to Release 7.5(1) for proper outbound option operation.
   - In order to support sequential dialing, and 10 telephone numbers per contact, the outbound option database has changed significantly, and requires you to re-import the campaign lists.
4. Create the Outbound Option database (if required) on the new Logger using SQL Enterprise Manager.
5. Use the EDMT to migrate the Logger database from the production Logger to the new Logger.
6. Export the ICM Logger registry from the production Logger, and import the registry to the new Logger.

   Note: Refer to Exporting and Importing the Registry (page 125) for additional information.
7. Run ICM setup.exe from the ICM/IPCC 7.5(1) CD on the new Logger. Choose to apply the automated hardening when prompted.
8. Using Domain Manager, add the Logger instance to the appropriate Active Directory Instance organizational unit.

   Note: This step only needs to be run if it is the first component to be upgraded to Release 7.5(1).

9. From ICM setup, edit the instance by inserting the new domain name (select the OU created in the previous step).
10. From ICM setup, edit the Logger component and make the necessary changes based on the environment in which the new Logger is to run.
11. Exit and then rerun setup. When the main setup screen appears, select **Upgrade All**.
12. Using ICM Service Control, set all ICM processes on the new Logger to **Manual Start**.
13. Reboot the Logger.
14. Migrate users from the production system to the new environment.

    For additional information, refer to the **Staging Guide, ICM/IPCC Enterprise/Hosted, ICM/IPCC Software Release 7.x(y)** (http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/microsf7/index.htm)
15. Install the latest ICM/IPCC 7.5(1) Maintenance Release and any required Engineering Specials on the new Logger.
16. If the Outbound Option is in use, re-import the customer contact lists and do-not-call lists (on the Side A or Side B Logger only).

    Note: The dialers and their associated PG must be upgraded to Release 7.5(1) for proper Outbound Option operation.
17. Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the new Logger.

Logger Common Ground Upgrade: Side A/B

Note: The following procedure is used to perform a Common Ground upgrade on both sides of the Logger. When upgrading Side A use the procedure as is. When upgrading Side B, simply replace “Side A” with “Side B” in the procedure.

Step 1 Disable configuration changes.

a. Set the HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\ICM\<instancename>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance key to 1 on both sides of the CallRouter in the system being upgraded.

Note: RouterA in the registry key above is RouterB on the Side B CallRouter.

b. Verify that configuration changes are prevented. The following message is displayed when attempting to save a configuration change:

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

Step 2 Using ICM Service Control, stop all ICM services on the Side A Logger, Distributor AW, and HDS.

Step 3 Using ICM Service Control, set all ICM services on the Side A Logger, Distributor AW, and HDS to **Manual Restart**.

Step 4 Using third party imaging or "ghost" software, perform a full system backup of the Side A Logger so that it can be restored if a critical failure occurs during the Common Ground upgrade process.

Step 5 Uninstall the Cisco Security Agent 4.0 Agent and the ICM Policy.

Step 6 Upgrade the Third Party Software such as virus protection software and VNC, or PC Anywhere.

Step 7 Reboot the Side A Logger.

Step 8 Install the Release 2.3(1) Support Tools agent.

Note: It is not necessary to uninstall older versions of the Support Tools agent.

Step 9 If the Outbound Option is in use, back up the Outbound Option private database using the SQL Server Enterprise Manager. The campaign manager is present on only one of the redundant Loggers, and needs to be upgraded on only that Logger.

Note:

- Dialers and their associated PG must be upgraded to Version 7.5(1) for proper outbound option operation.
- In order to support sequential dialing, and 10 telephone numbers per contact, the outbound option database has changed significantly, and requires you to re-import the campaign lists.

Step 10 Use the EDMT to migrate the Logger database.

Refer to Technology Refresh Migration Sequence (page 66) for additional information.

Step 11 Using the Domain Manager, add the Logger instance to the appropriate Active Directory Instance Organizational Unit.

Note: This step only needs to be run if it is the first component to be upgraded to Release 7.5(1).

Step 12 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD on the Logger. When the main setup screen appears, select **Upgrade All**.

Step 13 If the Active Directory domain is changing as part of the upgrade, run ICM setup.exe from the ICM/bin directory, edit the instance and insert the new domain name on the Side A Logger.

Step 14 While in ICM setup, edit the Logger component and review all entries

Step 15 Reboot the Logger.

Step 16 If necessary (for example, the domain changed), migrate users to the new environment.

For additional information, refer to the **Staging Guide, ICM/IPCC Enterprise/Hosted, ICM/IPCC Software Release 7.x(y)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_installation_guides_list.html)

Step 17 Install the latest ICM/IPCC 7.5(1) Maintenance Release and any required Engineering Specials on the new Logger.

Step 18 If the Outbound Option is in use, re-import the customer contact lists and do-not-call lists (on the Side A or Side B Logger only).

Note: The dialers and their associated PG must be upgraded to Version 7.5(1) for proper Outbound Option operation.

Step 19 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the new Logger.

Chapter 12

CallRouter Upgrade Procedures

CallRouter Pre-upgrade Preparation

Pre-upgrade preparation is an integral part of the upgrade process.

Perform the following on the CallRouter to assist in recovery in the event of a catastrophic upgrade failure:

1. Copy the Cisco registry key.
2. Copy the ICM/bin directory.

CallRouter Technology Refresh Upgrade: Side A/B

Note: The following procedure is used to perform a Technology Refresh upgrade on both sides of the Router. When upgrading Side A use the procedure as is. When upgrading Side B, simply replace “Side A” with “Side B” in the procedure.

Step 1 Export the ICM router registry from the production CallRouter, and import the registry to the new CallRouter.

Step 2 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD on the new CallRouter. Choose to apply the automated hardening when prompted.

Step 3 From ICM setup, edit the instance and insert the new domain name on the new CallRouter.

Step 4 From ICM setup, edit the CallRouter component and make the necessary changes based on the environment in which the new CallRouter is to be run.

Step 5 Using ICM Service Control, set all ICM processes on the new CallRouter to **Manual Start**.

Step 6 Exit and then rerun setup. When the main setup screen appears, select **Upgrade All**.

Step 7 Reboot the new CallRouter.

Step 8 Install the latest ICM/IPCC 7.5 Maintenance Release and any required Engineering Specials on the new CallRouter.

Step 9 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the new CallRouter.

Step 10 Upgrade any Network Gateways associated with NICs on the CallRouter. See Network Gateway Upgrades (page 159) for detailed instructions.

Note:

- DOS NICs are not supported by ICM/IPCC Release 7.5(1).
- **Important:** The Windows Firewall configuration scripts must be deployed before this server can accept network connections. This is done as part of the staging tasks.

CallRouter Common Ground Upgrade: Side A

Note: The following procedure is used to perform a Common Ground upgrade on both sides of the CallRouter. When upgrading Side A use the procedure as is. When upgrading Side B, simply replace “Side A” with “Side B” in the procedure .

Step 1 Using ICM Service Control, stop all ICM services on the Side A CallRouter.

Step 2 Using ICM Service Control, change all ICM services on the Side A CallRouter to **Manual Restart**.

Step 3 Using third party imaging or “ghost” software, perform a full system backup of the side A CallRouter server so that it can be restored should a critical failure occur during the common ground upgrade process.

Step 4 Uninstall the Cisco Security Agent 4.0 Agent and the ICM Policy.

Step 5 Upgrade the Third Party Software such as virus protection software and VNC, or PC Anywhere.

Step 6 Reboot the Side A CallRouter.

Step 7 Install the Release 2.3(1) Support Tools agent.

It is not necessary to uninstall older versions of the Support Tools agent.

Step 8 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD and select **Upgrade All** on the main setup screen to upgrade all ICM components on the Side A CallRouter.

Step 9 If the Active Directory domain is changing as part of the upgrade, run ICM setup.exe from the ICM/bin directory, edit the instance, and insert the new domain name on the Side A CallRouter.

Step 10 While in ICM setup, edit the CallRouter component and review all entries.

Step 11 Reboot the Side A CallRouter.

Step 12 Install the latest 7.5 Maintenance Release and any required Engineering Specials on the new CallRouter.

Step 13 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the new CallRouter.

Step 14 Upgrade any Network Gateways associated with NICs on the CallRouter. See Network Gateway Upgrades (page 159) for detailed instructions.

Note: DOS NICs are not supported by ICM/IPCC Release 7.5(1).

How to Bring Side A into Service

Once the steps outlined in the Administrative Workstation (AW) Upgrade Procedures (page 115), Logger Technology Refresh Upgrade: Side A/B (page 133), and CallRouter Technology Refresh Upgrade: Side A/B (page 139) are completed, follow the steps below to bring the ICM Side A Central Controller components into service:

Step 1 All components can “ping” public and private IP addresses as applicable to verify network connectivity between the upgraded ICM central controller components, but not to other ICM nodes in production. Shut down all non-upgraded AWs and the Side B CallRouter and Logger by stopping the ICM services on these components using ICM Service Control. Start the upgraded side.

Step 2 Using the ICM Service Control, manually start the ICM services on the Side A CallRouter and Logger, and the upgraded AW. Verify the basic operation of the Side A Central Controller components:

- General
  - Setup logs indicate no errors or failure conditions
  - AD domain has all users
  - Schema upgrade is successful for all databases (no loss of data integrity, or loss of data)
  - Registry changes are correct and match what is documented in setup logs
  - All component services start without errors
  - All general activities (accessing SQL Server, running third party software components like VNC or PCAnywhere, etc. are not stopped by CSA)
  - Calls are successfully processed

- CallRouter
  - Ccagent is in service but not connected to any peripheral gateways
  - Rtsvr is connected to the Primary AW
- Logger
  - Recovery process not required, no activity other than process start up
  - Users are in correct domain
  - Configuration information is passed to CallRouter
  - Replication process begins when HDS comes online
- HDS
  - AW indicates it is waiting for work
  - Replication process begins with no errors
- Security
  - Specified users are able to use configuration manager
  - Specified users are able to log in to WebView and can access both public and private reports (all previously existing reports are present)
- Script Editor
  - Users previous settings are present when application is opened
  - Validate All script yields same results as pre-upgrade test yielded
  - Scripts can be opened, edited, deleted or new scripts can be created
- ICMDBA
  - Import/Export functionality is present
  - Database space allocation and percent used are correct
- Support Tools
  - Can acquire logs, capture registry information, schedule collection of logs

Step 3 Using ICM Service Control, set the ICM services to **Autostart** on each of the upgraded ICM components.

Warning: Call processing is impacted until the next 3 steps are completed, and therefore they must be executed at an appropriate pre-planned time.

Note: At this time, default networking should occur.

Step 4 Using the ICM Service Control, stop the ICM Services the Side B Logger and the Side B CallRouter, and all AWs.

Step 5 Configure all other ICM components (PGs, gateways, NAMs, CICMs, multi-media components) to connect to the upgraded Side A Logger and Side A CallRouter.

Step 6 Using the ICM Service Control, start the ICM services on the upgraded Side A Logger, and Side A CallRouter. Start the ICM processes on the AW/HDS once its upgrade process is complete at any point at or after this step.

Step 7 Verify production system operation running with the upgraded Side A CallRouter and Side A Logger.

CallRouter Common Ground Upgrade: Side B

Repeat the steps in CallRouter Technology Refresh Upgrade: Side A/B (page 139) on the Side B CallRouter.

Note:

- **Important:** The Windows Firewall configuration scripts must be deployed before this server can accept network connections. This is done as part of the staging tasks.
- DOS NICs are not supported by ICM/IPCC Release 7.5(1).

Verify the basic operation of the B Side CallRouter and Side B Logger

---

Step 1 Manually synchronize Logger B to Logger A (with B being the last to be upgraded and before bringing it online) using ICMDBA.

Step 2 Start the side B CallRouter and Logger services.

Each service starts several process windows on the task bar of the local machine, each one an ICM program associated with the service. As each node starts up, it looks for the other server components and attempts to register with them. If you completed the ICM Setup and network testing successfully, no major errors should occur.

In order to add configuration data, the Central Controller and Admin Workstation(s) must be running. The ICM software loads an ICM Service Control tool on the desktop of each server used to control the services loaded on that machine.

Verify that the ICM Processes have no errors.

- CallRouters
  - Router: UP and synchronized with peer.

  - Ccagent: [In service, but not connected to any peripheral gateways.]
  - Rtsvr: [no connectivity to AW at this time.]
- Loggers
  - Logger: Connected to its respective database and synchronized with peer. MDS is in service.
  - Replication: [No connectivity to AW HDS at this time.]
  - Campaign Manager: [You see errors, no BA Dialer setup at this time.]

Step 3 Start AW (Distributor) Services

Start the Distributor Service within Cisco Service Control. Verify that the ICM Processes have no errors.

CallRouters

- Router: UP and synchronized with peer.
- Ccagent: [In service but not connected to any peripheral gateways.]
- Rtsvr: [Feed activated to AW.]

Loggers

- Logger: Connected to its respective database and synchronized with peer. MDS is in service.
- Replication: Connected to the AW.
- Campaign Manager: [You see errors, no BA Dialer setup at this time.]

Admin Workstation

- Updateaw: Displays "waiting for new work".
- Iseman: Listen thread waiting for client connection.
- Replication: Replication and recovery client connection initialized.
- Cms_jserver: Unable to initialize until the configuration is done.
- Cmsnode: Shutdown in progress, terminating.

Step 4 Settings for Production Environment

Validate the following settings from the system diagram for the Production Environment and make the required changes prior to placing the systems in production:

a. Clear Event logs.

b. Clear any Dr. Watson application errors.

c. Remove any diskettes, CD's or media from drives.

d. Make sure that all ICM Services are set to **Manual Start**. Services are not set to **Autostart** until after the implementation testing in the production environment.

Step 5 Using ICM Service Control, set the ICM services to **Autostart**on the upgraded Side B CallRouter and Logger.

Step 6 Using ICM Service Control, start the ICM services on the new Side B CallRouter and Logger.

If possible, once data synchronization is complete between the Loggers, cycle the ICM services on the Side A CallRouter and Side A Logger and verify that the Side B takes over and that the system continues to operate normally.

Step 7 Verify overall system operation.

Step 8 Enable configuration changes.

a. Set the HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance key to 0 on the Side A and Side B CallRouters of the system being upgraded.

Note: RouterA in the registry key above is RouterB on the Side B CallRouter.

b. Verify that configuration changes are possible.

Step 9 If the Outbound Option is in use, upgrade all Outbound Option dialers and their associated PGs per the procedures in Peripheral Gateway (PG) Upgrade Procedures (page 147).

Step 10 Upgrade any other Distributor AWs and/or HDSs using the steps documented in Administrative Workstation (AW) Upgrade Procedures (page 115).

CallRouter Common Ground Upgrade: Side B

Chapter 13

Peripheral Gateway (PG) Upgrade Procedures

PG Pre-upgrade Preparation

Pre-upgrade preparation is an integral part of the upgrade process.

Perform the following on all PGs to assist in recovery in the event of a catastrophic upgrade failure:

1. Copy the Cisco registry key.
2. Copy the ICM/bin directory.

Upgrading PGs

While different Peripheral Gateways (PGs) can be upgraded at different times, the A and B side of redundant PG pairs must be upgraded within the same maintenance window, along with associated CTI Servers, CTI OS servers, and Outbound Option dialers. For proper Outbound Option operation, all Outbound Option dialers must be upgraded during the same maintenance window as the Campaign Manager.

If a CAD version prior to 6.0 is connected to the PG being upgraded, both the CAD server and the associated CAD desktops must first be upgraded to a version compatible with ICM/IPCC 7.0 or later. CAD Version 7.0 requires CTI OS Release 7.0. CAD Version 7.0(1) requires CTI OS Version 7.0 SR3 or later. CAD Version 7.1(x) requires CTI OS 7.1(x). CAD 7.2(x) requires CTI OS 7.2(x). CAD 7.5 requires CTI OS 7.5(1).

For CallManager PGs and Generic PGs with CallManager PIMs, CallManager clusters must be upgraded to Version 4.0, 5.0, 5.1, 6.0, or 6.1 prior to upgrading the PG to ICM/IPCC Release 7.5(1). Versions of CallManager earlier than 4.0 are not supported by ICM/IPCC Release 7.5(1). IP IVRs associated with the CallManager must also be upgraded to a compatible version.

ICM/IPCC 7.0 introduced a new PG type, called the IPCC System PG. In ICM/IPCC 7.0 or later, this PG supports a CallManager PIM and multiple VRU PIMs while appearing as a single peripheral to the ICM. There is no automated upgrade to the IPCC System PG model from a system using separate CallManager and VRU PGs, or a system using a Generic PG with CallManager and VRU PIMs.

ICM/IPCC 7.5(1) can operate with PGs at ICM Release 5.0(x), 6.0(0), 7.0(x), 7.1(x), or 7.2(x).

The version of CTI OS must be aligned with the PG version, for example:

- PGs at ICM Release 7.0(x) require CTI OS Release 7.0(x).
- PGs at ICM Release 7.1(x) require CTI OS Release 7.1(x).
- PGs at ICM Release 7.2(x) require CTI OS Release 7.2(x).

This document assumes that if CTI Gateways (CGs) are in use, they are collocated on the same server as the PG. The CTI Gateway primary process is the CTI Server. The CTI OS Server is a separate component, and may be collocated, or on a separate server from the PG.

PG Technology Refresh Upgrade

Step 1 Set up the new Side A and Side B PG servers as outlined in Setting up the Hardware (page 35).

Step 2 Using the ICM Service Control, stop all ICM and CTI OS services on the Side A production PG.

Step 3 Export the ICM registry from production PG, and import the registry to the new PG.

Note: Refer to Exporting and Importing the Registry (page 125) for additional information.

Step 4 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD on the new side A PG. Choose to apply the automated hardening when prompted.

Step 5 From ICM setup, edit all instances on the new server and insert the new domain name.

Step 6 From ICM setup, edit all ICM components (PG, dialer, and CTI Server) on the new server and make the necessary changes based on the environment in which the new PG is to run.

Step 7 Exit and then rerun setup. When the main setup screen appears, select **Upgrade All**.

Step 8 If CTI OS server is to be installed on the same server as the PG, run setup on the CTI OS 7.5(1) CD to install the CTI OS server. Input the appropriate domain name and other configuration elements as they apply to the new environment.

Step 9 If this is a CallManager PG or a Generic PG with a CallManager PIM, upload the JTAPI Client from CallManager.

How to Install the Cisco JTAPI Client on the Generic IPCC PG

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

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

a. Open a browser window on the PG machine.

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

c. Enter the user name and password that you created when installing and configuring Cisco CallManager (Lab Value: cm_pg_user).

d. Choose **Application** > **Install Plug-ins**.

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

f. Choose **Run this program from its current location**. Click **OK**.

g. On the Security Warning box, click **Yes** to install.

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

i. Click **Finish**.

j. Reboot the machine to ensure proper operation of JTAPI.

For additional information, refer to **IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition, Cisco IPCC Enterprise Edition Release 7.5(1)** (http://www.cisco.com/univercd/cc/td/doc/product/icm/ipccente/ipcc70d/ipcccor7/index.htm)

Step 10 Using ICM Service Control, set the ICM and CTI OS processes on the new Side A PG to **Manual Start**.

Step 11 Reboot the PG.

Step 12 Install the latest ICM/IPCC 7.5 Maintenance Release and any required Engineering Specials on the new PG.

Step 13 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the new PG.

Step 14 If there are Outbound Option dialers associated with the PG pair being upgraded which are on separate servers, upgrade all of them now.

PG Common Ground Upgrade

Step 1 Using ICM Service Control, stop all ICM and CTI OS services on the Side A PG.

Step 2 Using ICM Service Control, change all ICM and CTI OS services on the Side A PG to **Manual Restart**.

Step 3 Using third party imaging or "ghost" software, perform a full system backup of the side A Peripheral Gateway server so that it can be restored should a critical failure occur during the common ground upgrade process.

Step 4 Uninstall the Cisco Security Agent 4.0 Agent and the ICM Policy.

Step 5 Upgrade Third Party software such as virus protection software and VNC or PC Anywhere.

Step 6 Reboot the Side A PG.

Step 7 Install the Release 2.3(1) Support Tools agent. It is not necessary to uninstall older versions of the Support Tools agent.

Step 8 Using the Domain Manager, add the PG instance to the appropriate Active Directory Instance Organizational Unit.

Step 9 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD and select **Upgrade All** on the main setup screen to upgrade all ICM components on the Side A PG.

Step 10 If the Active Directory domain is changing as part of the upgrade, run ICM setup.exe from the ICM/bin directory, edit the instance and insert the new domain name on the Side A PG.

Step 11 While in ICM setup, edit the PG component and review all entries.

Step 12 If CTI OS is collocated on the same server as the PG, run setup.exe from the CTI OS 7.5(1) CD to install CTI OS 7.5(1) on side A. It is not necessary to uninstall previous releases of CTI OS.

Step 13 If this is a CM PG or a Generic PG with a CallManager PIM, upload the JTAPI Client from CallManager.

How to Install the Cisco JTAPI Client on the Generic IPCC PG

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

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

a. Open a browser window on the PG machine.

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

c. Enter the user name and password that you created when installing and configuring Cisco CallManager (Lab Value: cm_pg_user).

d. Choose **Application > Install Plug-ins**.

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

f. Choose **Run this program from its current location**. Click **OK**.

g. On the Security Warning box, click **Yes** to install.

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

i. Click **Finish**.

j. Reboot the machine to ensure proper operation of JTAPI.

For additional information, refer to **IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition, Cisco IPCC Enterprise Edition Release 7.5(1)** (http://www.cisco.com/univercd/cc/td/doc/product/icm/ipccente/ipcc70d/ipcccor7/index.htm)

Step 14 Install the latest ICM/IPCC 7.5 Maintenance Release and any required Engineering Specials on the Side A PG.

Step 15 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the Side A PG.

Step 16 If there are Outbound Option dialers associated with the PG pair being upgraded which are on separate servers, upgrade all of them now.

Upgrading Outbound Option Dialers

Because of the added capability and increased number of contacts supported by the Outbound Option in ICM/IPCC Release 7.5(1), it is necessary to re-import the contact and do-not call lists when upgrading.

Information regarding which contacts have been called and which are yet to call on in-process outbound campaigns is lost during the upgrade, so the timing of the upgrade must be planned accordingly. In addition, the Outbound Option dialers and their associated PGs must be upgraded to Release 7.5(1) for proper Outbound Option operation.

Outbound Option Dialer Technology Refresh Upgrade

Step 1 Set up the new server as outlined in Setting Up the Hardware (page 35).

Step 2 Using the ICM Service Control, stop all ICM services on the production dialer being replaced.

Step 3 Export the ICM registry from production dialer, and import the registry to the new dialer.

Note: Refer to Exporting and Importing the Registry (page 125) for additional information.

Step 4 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD on the new dialer. Apply the automated hardening when prompted.

Step 5 From ICM setup, edit all instances on the server and insert the new domain name.

Step 6 From ICM setup, edit all ICM components on the server and make the necessary changes based on the environment in which the new dialer is to run.

Step 7 Exit and then rerun setup. When the main setup screen appears, select **Upgrade All**.

Step 8 Using ICM Service Control, set the ICM processes on the new dialer to **Manual Start**.

Step 9 Reboot the new dialer.

Step 10 Install the latest ICM/IPCC 7.5 Maintenance Release and any required Engineering Specials on the new dialer.

Step 11 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the new dialer.

Step 12 Using ICM Service Control, start the ICM processes on the new dialer.

Step 13 Using ICM Service Control, set the ICM processes on the new dialer to Automatic Start.

Outbound Option Dialer Common Ground Upgrade

Step 1 Using ICM Service Control, stop all ICM services on the dialer.

a. Using ICM Service Control, change all ICM services on the dialer to **Manual Restart**.

b. Using third party imaging or “ghost” software, perform a full system backup of the dialer server so that it can be restored should a critical failure occur during the common ground upgrade process.

c. Uninstall the Cisco Security Agent 4.0 Agent and the ICM Policy.

d. Upgrade Third Party software such as virus protection software, VNC, or PCAnywhere.

e. Reboot the dialer.

f. Install the Release 2.3(1) Support Tools agent. It is not necessary to uninstall older versions of the Support Tools agent.

g. Using the Domain Manager, add the dialer instance to the appropriate Active Directory Instance Organizational Unit.

h. Run ICM setup.exe from the ICM/IPCC 7.5(1) CD and select **Upgrade All** on the main setup screen to upgrade all ICM components on the dialer.

i. If the Active Directory domain is changing as part of the upgrade, run ICM setup.exe from the ICM/bin directory, edit the instance and insert the new domain name on the dialer.

j. While in ICM setup, edit the dialer component and review all entries.

k. Reboot the dialer.

l. Install the latest 7.5 Maintenance Release and any required Engineering Specials on the dialer.

m. Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the dialer.

Step 2 If there are CTI OS servers associated with the PG pair being upgraded which are on separate servers, upgrade half of them now.

Upgrading Standalone CTI OS Servers

If there are CTI OS servers associated with the PG pair being upgraded that are on separate servers, upgrade half of them now.

Standalone CTI OS Server Technology Refresh Upgrade

Step 1 Set up the new CTI OS server as outlined in Setting up the Hardware (page 35).

Step 2 Using the ICM Service Control, stop all CTI OS services on the CTI OS server being upgraded.

Step 3 Export the ICM registry from production CTI OS server, and import the registry to the new CTI OS Server.

Note: Refer to Exporting and Importing the Registry (page 125) for additional information.

Step 4 Run setup on the CTI OS 7.5(1) CD to install the CTI OS server. Input the appropriate domain name and other configuration elements as they apply to the new environment.

Step 5 Using ICM Service Control, set the CTI OS processes on the new CTI OS Server to **Manual Start**.

Step 6 Reboot the CTI OS Server.

Step 7 Install the latest CTI OS 7.5 Maintenance Release and any required Engineering Specials on the new CTI OS Server.

Step 8 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the new CTI OS Server.

Step 9 Using ICM Service Control, set the CTI OS processes on the new CTI OS Server to **Automatic Start**.

Step 10 Adjust the clients of the original CTI OS Server to connect to the new CTI OS Server.

Step 11 Shut down the original CTI OS Server, bring the new CTI OS Server online, and verify proper system operation.

Step 12 If CTI OS server is collocated on the PG, modify the CTI OS clients to connect to the new Side A PG/CTI OS server.

Note: Call processing for the Peripheral being upgraded is affected until the next four steps are completed.

Step 13 Using ICM Service Control, stop the ICM and CTI OS services on the Side B production PG.

Step 14 Using ICM Service Control, start all ICM and CTI OS services on the new Side A PG.

Step 15 Using ICM Service Control, set all of the ICM and CTI OS processes on the new Side A PG to **Automatic Start**.

Step 16 Verify proper operation of the peripheral running on the new Side A PG (call flows, CTI desktops and other applications, Outbound Option dialer).

Step 17 Repeat steps 2 through 16 to upgrade the Side B PG.

Step 18 Upgrade any remaining associated CTI OS servers on separate servers.

Standalone CTI OS Server Common Ground Upgrade

Step 1 Using ICM Service Control, stop all CTI OS services on the server being upgraded.

Step 2 Using ICM Service Control, change all CTI OS services to **Manual Restart**.

Step 3 Using third party imaging or “ghost” software, perform a full system backup of the CTI OS server so that it can be restored should a critical failure occur during the Common Ground upgrade process.

Step 4 Uninstall the Cisco Security Agent 4.0 Agent and the ICM Policy.

Step 5 Upgrade Third Party software such as virus protection software and VNC or PCAnywhere.

Step 6 Reboot the CTI OS Server.

Step 7 Install the Release 2.3(1) Support Tools agent. It is not necessary to uninstall older versions of the Support Tools agent.

Step 8 Using the Domain Manager, add the CTI OS Server to the appropriate Active Directory Instance Organizational Unit.

Step 9 Run setup on the CTI OS 7.5(1) CD to install the CTI OS server. Input the appropriate domain name and other configuration elements as they apply to the new environment.

Step 10 While in CTI OS setup, review all entries and update as required.

Step 11 Reboot the CTI OS Server.

Step 12 Install the latest ICM/IPCC 7.5 Maintenance Release and any required Engineering Specials on the CTI OS Server.

Step 13 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the CTI OS Server.

Step 14 Using ICM Service Control, change all CTI OS services to **Automatic Restart**.

Step 15 Bring the upgraded CTI OS server online and verify proper system operation.

Note: Call processing for the Peripheral being upgraded is affected until the next four steps are completed.

Step 16 Using ICM Service Control, stop the ICM and CTI OS services on the Side B PG.

Step 17 Using ICM Service Control, start all ICM and CTI OS services on the Side A PG.

Step 18 Using ICM Service Control, set all of the ICM and CTI OS processes on the Side A PG to **Automatic Start**.

Step 19 Verify proper operation of the peripheral running on the upgraded Side A PG (call flows, CTI desktops and other applications, Outbound Option dialer).

Step 20 Using third party imaging or “ghost” software, perform a full system backup of the side B Peripheral Gateway server so that it can be restored should a critical failure occur during the common ground upgrade process.

Step 21 Uninstall the Cisco Security Agent 4.0 Agent and the ICM Policy.

Step 22 Upgrade Third Party software such as virus protection software and VNC or PC Anywhere.

Note: Perform Step 23 through Step 36 (inclusive) on the Side B PG.

Step 23 Reboot the Side B PG.

Step 24 Install the Release 2.3(1) Support Tools agent. It is not necessary to uninstall older versions of the Support Tools agent.

Step 25 Using the Domain Manager, add the PG instance to the appropriate Active Directory Instance Organizational Unit.

Step 26 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD and select Upgrade All on the main setup screen to upgrade all ICM components on the Side B PG.

Step 27 If the Active Directory domain is changing as part of the upgrade, run ICM setup.exe from the ICM/bin directory, edit the instance and insert the new domain name on the Side B PG.

Step 28 While in ICM setup, edit the PG component and review all entries.

Step 29 If CTI OS is collocated on the same server as the PG, run setup.exe from the CTI OS 7.5(1) CD to install CTI OS 7.5(1) on side B. It is not necessary to uninstall previous releases of CTI OS.

Step 30 If this is a CM PG or a Generic PG with a CallManager PIM, upload the JTAPI Client from CallManager.

How to Install the Cisco JTAPI Client on the Generic IPCC PG

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

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

To install the Cisco JTAPI Client:

a. Open a browser window on the PG machine.

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

c. Enter the user name and password that you created when installing and configuring Cisco CallManager.

Lab Value: cm_pg_user

d. Choose **Application** > **Install Plug-ins**.

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

f. Choose **Run this program from its current location**. Click **OK**.

g. On the Security Warning box, click **Yes** to install.

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

i. Click **Finish**.

j. Reboot the machine to ensure proper operation of JTAPI.

For additional information, refer to **IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition, Cisco IPCC Enterprise Edition Release 7.5(1)** (http://www.cisco.com/univercd/cc/td/doc/product/icm/ipccente/ipcc70d/ipcccor7/index.htm)

Step 31 Install the latest ICM/IPCC 7.5 Maintenance Release and any required Engineering Specials on the Side B PG.

Step 32 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the Side B PG.

Step 33 Upgrade any remaining associated CTI OS servers on separate servers.

Chapter 14

Network Gateway Upgrade Procedures

Gateway Technology Refresh Upgrade

How to perform a TR upgrade on an AT&T or a SS7-ITU Gateway

Note: DOS NICs are not supported by ICM/IPCC Release 7.5(1).

Step 1 Set up the new server as outlined in Setting Up the Hardware (page 35).

Step 2 Using the ICM Service Control, stop all ICM services on the production gateway being replaced.

Step 3 Install the PCI card in the new server.

Step 4 Import the Cisco systems inc. reg key from the existing Gateway to the to the new 7.5(1) systems.

Step 5 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD on the new gateway, using edit to make necessary changes to hostnames, IPs etc.

Step 6 Check the PCI card button.

Step 7 Apply the automated hardening when prompted.

Step 8 From ICM setup, edit all instances on the server and insert the new domain name.

Step 9 From ICM setup, edit all ICM components on the server and make the necessary changes based on the environment in which the new gateway is to run.

Step 10 Exit setup, then rerun setup from the media (do not reboot). When the main setup screen appears, select **Upgrade All**.

Step 11 Reboot the server.

Step 12 Allow the system to find the "Fatboy" PCI card. When Windows asks, the PCI drivers are located at: **`ICM Installation disk \Drivers\w2k\PCI\SS7PCIDrivers.sys`**.

Step 13 Reboot when asked.

Step 14 Using ICM Service Control, set the ICM processes on the new gateway to **Manual Start**.

Step 15 Reboot the new gateway.

Step 16 Install the latest ICM/IPCC 7.5 Maintenance Release and any required Engineering Specials on the new gateway.

Step 17 **Note:** If the same links are being used, no changes need to be made to the SS7 configuration. If new or different links are being used, the SS7.cfg application must be run to make the necessary changes.

Step 18 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the new gateway.

Step 19 Using ICM Service Control, start the ICM processes on the new gateway.

Step 20 Using ICM Service Control, set the ICM processes on the new gateway to **Automatic Start**.

Gateway Common Ground Upgrade

How to perform a TR upgrade on an AT&T or a SS7-ITU Gateway

Note: DOS NICs are not supported by ICM/IPCC 7.5(1).

Step 1 Using ICM Service Control, stop all ICM services on the gateway.

Step 2 Using ICM Service Control, change all ICM services on the gateway to **Manual Restart**.

Step 3 Using third party imaging or “ghost” software, perform a full system backup of the gateway server so that it can be restored should a critical failure occur during the Common Ground upgrade process.

Step 4 Uninstall the Cisco Security Agent 4.0 Agent and the ICM Policy.

Step 5 Upgrade Third Party software such as virus protection software, VNC, or PCAnywhere.

Step 6 Reboot the gateway.

Step 7 Install the Release 2.3(1) Support Tools agent. It is not necessary to uninstall older versions of the Support Tools agent.

Step 8 Using the Domain Manager, add the dialer instance to the appropriate Active Directory Instance Organizational Unit.

Step 9 Run ICM setup.exe from the ICM/IPCC 7.5(1) CD and select **Upgrade All** on the main setup screen to upgrade all ICM components on the dialer.

Step 10 If the Active Directory domain is changing as part of the upgrade, run ICM setup.exe from the ICM/bin directory, edit the instance and insert the new domain name on the gateway.

Step 11 While in ICM setup, edit the Gateway component and review all entries.

Step 12 Reboot the gateway.

Step 13 Install the latest ICM/IPCC 7.5 Maintenance Release and any required Engineering Specials on the gateway.

Step 14 Install Cisco Security Agent 5.2 with the latest compatible CSA Agent Policy on the gateway.

Chapter 15

Upgrading a Localized ICM/IPCC System

Localization Upgrade Considerations

Note: Changing the Windows operating system, SQL Server, or ICM/IPCC software from one language to another is not supported during the upgrade process.

Upgrading from ICM/IPCC 7.0(x), 7.1(x), or 7.2(x)

There is no language selection in ICM/IPCC 7.5(1). Run ICM 7.5(1) Setup.exe then select **Upgrade All**. This results in the system checking the language setting for the 7.0(x), 7.1(x), or 7.2(x) system being upgraded, then upgrading all the language components to the same language in ICM 7.5(1).

Chapter 16

CIS Upgrade Procedures

There are no new releases of the Cisco CIS components (Cisco Email Manager, Cisco Collaboration Server, Cisco Media Blender, and Dynamic Content Adapter) in the 7.5(1) release cycle.

Chapter 17

CTI OS Agent and Supervisor Desktop Upgrade Procedures

CTI OS Agent and Supervisor Desktop Technology Refresh Upgrade

Technology Refresh upgrades are no different than fresh installations, except that the original desktop is taken off-line. Refer to the **CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions** (http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod_installation_guides_list.html).

Note: Customized desktops may have different upgrade procedures which are beyond the scope of this document.

CTI OS Agent and Supervisor Desktop Common Ground Upgrade

Upgrading the standard CTI OS Agent and Supervisor Desktops without upgrading the hardware (CG upgrade) involves the following:

Step 1 Stop the CTI OS Agent or Supervisor Desktop application that is running on the machine.

Step 2 Run the CTI OS Client install from the ICM/IPCC 7.5(1) CD, updating configuration data as prompted.

Step 3 Reboot the machine if directed to.

Chapter 18

Cisco Agent Desktop (CAD) Upgrade Procedures

CAD 7.5 is integrated as follows:

Table 6:

CAD Version	Unified CM Version	Unified SCCE Version
7.5(1)	4.1, 4.2, 5.0, 6.0	7.5(1)

Note: If you are upgrading a replicated system, you must shut down replication before doing an upgrade. After you finish the upgrade, re-establish replication.

Upgrading from CAD 7.5 from CAD 6.0(2)

If you are upgrading to CAD 7.5 from CAD 6.0(2), you must complete the following steps in the order shown.

Step 1 Back up your configuration data using the CAD backup and restore utilities for the version you are upgrading.

Step 2 Uninstall the previous version of CAD.

Step 3 Install CAD 7.5 and restore the data you backed up during the installation process.

If you are upgrading to CAD 7.5 from CAD 7.0, 7.1, or 7.2, you can install CAD 7.5 directly over the previous version. You can also upgrade a previous version of CAD 7.5 to the current version of CAD 7.5 by installing the current version over the previous version.

Note:

- It is recommended that you upgrade the CAD services only when no CAD users (agents, supervisors, and administrators) are logged into the system. If users are logged in, they may receive error messages when the services go offline during the upgrade.

- In CAD 7.1 or higher, reason codes are created and maintained in Unified SCCE. Any reason codes that you created using Desktop Administrator in previous versions of CAD will be lost in an upgrade. To continue using previously-created reason codes, re-create them in Unified SCCE.

Refer to the *Cisco CAD Installation Guide* for detailed instructions for upgrading from previous versions of CAD.

Chapter 19

Remote Monitoring System (RMS) Upgrade Procedures

Upgrading Listener Clients that Dial in via Modem

Note: Before upgrading the LGMapper server to Windows Server 2003, as a precaution, back up the LGMapper_Alarms and LGArchiver_Alarms. Also, stop and set to manual (or disabled) the LGMapper and LGArchiver services.

The following steps must be performed if the system supports clients dialing in via modem to talk to the Listener application:

Step 1 Configure Microsoft RAS on the current Listener server (Release 2.0 or 2.0 SR1) for TCP/IP and NetBEUI. This enables the new ICM 7.5(1) Loggers to dial in. In addition, this is a needed preparation before reconfiguring earlier ICM Logger versions to TCP

Step 2 Install new message files on the AlarmTracker Client machines by running SDDSN setup from the latest ICM setup CD.

Step 3 Configure all Loggers to phone home using TCP. This must be done before upgrading the Listener server to Windows 2003. This should be done over time to allow a window where Loggers still use NetBEUI to dial in.

Upgrading RMS Components to Version 2.1

The procedure to upgrade the RMS components to Release 2.1 is as follows:

Step 1 Disconnect all AlarmTracker clients and exit the application.

Step 2 Stop the Listener Service on the Listener system.

Step 3 Disable CSA and stop the CSA service on the servers being upgraded.

Step 4 Stop the LGMapper and LGArchiver services on the Mapper server.

Step 5 Run Listener Setup on the Listener system.

Step 6 Run LGMapper Setup on the Mapper system.

Step 7 Run AlarmTracker Client Setup on the Client systems.

Step 8 Start the Listener service on the Listener systems.

Step 9 Start the LGMapper service on the Mapper servers.

Step 10 Start the LGArchiver service on the Mapper servers.

Step 11 Start the clients and connect them to the Mapper servers.

Step 12 Restart the CSA service and enable CSA on the upgraded servers.

Windows 2003 Upgrade on Listener and Mapper Servers

RMS should be upgraded to Release 2.1 before upgrading the OS to Windows 2003. If using dial-up (RAS), all Loggers must already be configured for TCP over RAS.

Prior to beginning to upgrade the operating system:

Step 1 Disconnect all AlarmTracker clients and exit the application.

Step 2 Stop the Listener Service on the Listener system.

Step 3 Disable CSA and stop the CSA service on the servers being upgraded.

Once the operating system on the Listener and Mapper servers have been upgraded:

Step 4 Start the Listener service on the Listener systems.

Step 5 Start the LGMapper service on the Mapper servers.

Step 6 Start the LGArchiver service on the Mapper servers.

Step 7 Start the clients and connect them to the Mapper servers.

Step 8 Restart the CSA service and enable CSA on the upgraded servers.

Chapter 20

Database Tasks

This chapter contains the following topics:

How to set the Logger or HDS database data file size for maximum growth using SQL Enterprise Manager

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

Step 2 Expand Microsoft SQL Servers by clicking the + icon next to it.

Step 3 Expand SQL Server Group by clicking the + icon next to it.

Step 4 Expand server name where the destination database is to be created by clicking the + icon next to it.

Step 5 In the Databases folder, drill down and select the appropriate database.

Step 6 Right-click on the selected database and select **Properties**.

Step 7 Select the **Data Files** tab.

Step 8 Set file to **Automatically grow file**.

Step 9 In the Maximum file size section, click **Unrestrict file growth** (in MB).

How to Determine the Size of an ICM Database

When migrating from an older ICM/IPCC release to a newer ICM/IPCC release, you need to lookup the database size of the existing ICM database. This number is used later in the process to create an ICM database of the same size. This value may be increased depending on planned ICM 7.5(1) usage patterns. Find the database size either by launching the ICMDBA program or by launching the Microsoft ISQL_w program on the SQL Server.

Using ICMDBA

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 **icmdba**.

Step 4 Drill down to the Logger/HDS database.

Step 5 Right-click **cust_sideX** and select **Properties** to observe the database size.

Using SQL Enterprise Manager

Step 1 On the SQL Server systems, launch **Start > Programs > Microsoft SQL Server 2005 > SQL Server Management Studio**.

Step 2 Enter the required database connection information:

- Make sure that the current system name is selected.
- Select **Windows Authentication**.

Step 3 Click **Connect**.

Step 4 The Microsoft SQL Server Management Studio application opens. Navigate to **Databases > System Databases > master**.

Step 5 Right click on the master database and select **New Query**.

Step 6 On the right side of the window, a query window opens. Enter **EXECUTE sp_helpdb** into the Query window and execute the script by clicking the **green arrow** or by pressing **F5**.

Step 7 Note the value located in the db_size column for the ICM database.

Step 8 Exit the Microsoft SQL Server Management Studio program. If you are asked to save changes to your query, answer **No**.

How to Set the tempdb Database Size

The size and configuration of the tempdb database during data migration differs for the parameters used in a production system. This section describes how to set tempdb for each case.

For Data Migration

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

Step 2 Expand Databases by clicking on the + icon, right-click on the tempdb database, and select **Properties**.

Step 3 Click on the **Data Files** tab. Set the following parameters:

- Space Allocated must be at least **1400 MB**.
- Set **Automatically grow files**.
- Set **Unrestricted file growth**.

Step 4 Click on the **Transaction Log** tab. Set the following parameters:

- Space Allocated must be at least **400 MB**.
- Set **Automatically grow files**.
- Set **Unrestricted file growth**.

Step 5 Click **OK**.

Step 6 Close SQL Enterprise Manager.

For Production Systems

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

Step 2 Expand Databases by clicking on the + icon, right-click on the tempdb database, and select **Properties**.

Step 3 Click on the **Data Files** tab. Set the following parameters:

- Space Allocated must be at least **100 MB**. The allocated space may be significantly larger after data migration. If so, shrink the file down to 100 MB.
- Set **Automatically grow files**.
- Set Maximum file size to **500 MB**.

Step 4 Click on the **Transaction Log** tab. Set the following parameters:

- Space Allocated must be at least **50 MB**.
- Disable **Automatically grow files**.

Step 5 Click **OK**.

Step 6 Close SQL Enterprise Manager.

Chapter 21

Upgrade Checklists

Select one of the following checklists. Make your choice based on the upgrade procedure that most fits your ICM/IPCC system upgrade requirements. Modify the checklist as necessary, to match the upgrade requirements of your specific system.

This chapter contains the following topics:

Technology Refresh Upgrade Checklists

Select the appropriate Technology Refresh checklist for your ICM/IPCC system upgrade.

Table 7: Production HDS/Distributor AW Upgraded in Parallel with the Central Controller Upgrade Maintenance Window

Warning: In order to complete an upgrade successfully, the order of upgrade as defined in this checklist MUST be followed.

Step/Completed	Action/Reference	Comments
1. Upgrade the production system to the required baseline.	Complete the applicable baseline requirements: • Ensure all ICM nodes are at ICM/IPCC Release 7.0(x), ICM/IPCC Release 7.1(x), or ICM/IPCC Release 7.2(x). • Ensure all ICM/IPCC nodes are running Windows 2000 SP4 or Windows 2003. • Ensure the Logger and HDS are running SQL Server 2000 or SQL Server 2005, as appropriate, including the latest supported service pack.	

Step/Completed	Action/Reference	Comments
	• Ensure the CAD is at Release 6.0, 7.0, 7.1, or 7.2 on Windows 2000 Server SP4 or Windows 2000 Advanced Server. • Ensure the CTI OS desktops are at Version 7.0(x), 7.1(x), or 7.2(x). • Ensure CEM, CCS, CMB at Version 6.0, 7.0, or 7.5. • Ensure DCA is at Version 2.1. • Ensure CCM is at Version 4.1, 4.2, 5.0, or 6.0, with the compatible IP IVR or CVP (ISN) version. • Ensure all ACDs are at a version compatible with ICM/IPCC 7.5(1). • Ensure the hardware meets BOM specifications. • Create and configure the Active Directory environment for ICM/IPCC. • Run the Windows firewall configuration scripts to enable network connectivity. • Ensure the ICM/IPCC Support Tools Server is upgraded to Version 2.3(1). • Perform a backup of the existing servers and verify the backups. For additional information refer to Baseline Requirements (page 21).	
2. Create the Active Directory environment.	AD considerations for upgrade: • Migrate users from the old domain to the new domain. • Put the new servers in the Active Directory domain in the appropriate ICM OU. • Validate IP connectivity and remote access. • If the AD domain controller is on the Logger, migrate the domain controller roles to new non-ICM servers. **Note:** Refer to "Migrating Active Directory and DNS to a Non-ICM Server" for additional information. • Bring up the new domain controllers on the domain in which the ICM operates.	

Step/Completed	Action/Reference	Comments
	• Transfer any applicable flexible single master operations (FSMO) roles. • Demote the domain controller on the production Logger to a member server. For additional information refer to Active Directory and DNS Considerations for Upgrades (page 51).	
3. Set up the new hardware.	Before performing a TR upgrade: • Install Windows 2003 and the latest service pack. • Deploy the Windows Firewall scripts. • Install SQL Server 2000 or 2005, as appropriate, including the latest supported service pack. • Install Release 2.3(1) Support Tools Agent. • Install the required Third Party software. • Install the newly deployed servers. • Verify system conditions using the EDMT. For additional information see Setting Up the Hardware (page 35).	
4. Set up a temporary 7.5(1) HDS/Distributor AW.	Refer to Setting Up a Temporary ICM/IPCC 7.5(1) AW/HDS (page 126).	
Start of Central Controller Upgrade Maintenance Window	**********	**********
5. Upgrade the Side A HDS/Distributor AW.	Refer to Distributor AW/HDS Technology Refresh Upgrade (page 119).	
6. Upgrade the Side A Logger.	Refer to Logger Technology Refresh Upgrade: Side A/B (page 133).	
7. Upgrade the Side A CallRouter.	Refer to CallRouter Technology Refresh Upgrade: Side A/B (page 139).	
8. Install the WebView server(s) if not collocated on the AW/HDS.	Refer to **WebView Installation Guide**[5]	
9. Bring down the production system (CallRouters, Loggers, and AWs). Bring up the new Side A CallRouter and Logger.	None.	

5) http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/report7/index.htm

Step/Completed	Action/Reference	Comments
Point the temporary HDS/Distributor AW, PGs, and CIS components to the new CallRouter & Logger in the new domain.		
10. Upgrade the Side B CallRouter.	Refer to CallRouter Technology Refresh Upgrade: Side A/B (page 139).	
11. Upgrade the Side B Logger.	Refer to Logger Technology Refresh Upgrade: Side A/B (page 133).	
End of Central Controller Upgrade Maintenance Window	**********	**********
12. Upgrade the Side B HDS/Distributor AW.	Refer to Distributor AW/HDS Technology Refresh Upgrade (page 119).	
13. Bring up the Upgraded the Side A HDS/Distributor AW S, when available, at any point after Step 8.	None.	
14. Bring up the Upgraded the Side B HDS/Distributor AW.	None.	
15. Upgrade the AWs, PGs, RMS, and CIS components.	Refer to: • Administrative Workstation (AW) Upgrade Procedures (page 115) • PG Technology Refresh Upgrade (page 148) • Remote Monitoring System (RMS) Upgrade Procedures (page 171) • CIS Upgrade Procedures (page 165)	

Table 8: Production HDS/Distributor AW Upgraded before the Central Controller Upgrade Maintenance Window

Warning: In order to complete an upgrade successfully, the order of upgrade as defined in this checklist MUST be followed.

Step/Completed	Action/Reference	Comments
1. Upgrade the production system to the required baseline.	Complete the applicable baseline requirements: • Ensure all ICM nodes are at ICM/IPCC Release 7.0(x), ICM/IPCC Release 7.1(x), or ICM/IPCC Release 7.2(x). • Ensure all ICM/IPCC nodes are running Windows 2000 SP4 or Windows 2003.	

Step/Completed	Action/Reference	Comments
	• Ensure the Logger and HDS are running SQL Server 2000 or SQL Server 2005, as appropriate, including the latest supported service pack. • Ensure the CAD is at Release 6.0, 7.0, 7.1, or 7.2 on Windows 2000 Server SP4 or Windows 2000 Advanced Server. • Ensure the CTI OS desktops are at Version 7.0(x), 7.1(x), or 7.2(x). • Ensure CEM, CCS, CMB at Version 6.0, 7.0, or 7.5. • Ensure DCA is at Version 2.1. • Ensure CCM is at Version 4.1, 4.2, 5.0, or 6.0, with the compatible IP IVR or CVP (ISN) version. • Ensure all ACDs are at a version compatible with ICM/IPCC 7.5(1). • Ensure the hardware meets BOM specifications. • Create and configure the Active Directory environment for ICM/IPCC. • Run the Windows firewall configuration scripts to enable network connectivity. • Ensure the ICM/IPCC Support Tools Server is upgraded to Version 2.3(1). • Perform a backup of the existing servers and verify the backups. For additional information refer to Baseline Requirements (page 21).	
2. Create the Active Directory environment.	AD considerations for upgrade: • Migrating users from the old domain to the new domain. • Put the new servers in the Active Directory domain in the appropriate ICM OU. • Validate IP connectivity and remote access. • If the AD domain controller is on the Logger, migrate the domain controller roles to new non-ICM servers. **Note:** Refer to "Migrating Active Directory and DNS to a Non-ICM Server" for additional information.	

Step/Completed	Action/Reference	Comments
	• Bring up the new domain controllers on the domain in which the ICM operates. • Transfer any applicable flexible single master operations (FSMO) roles. • Demote the domain controller on the production Logger to a member server. For additional information refer to Active Directory and DNS Considerations for Upgrades (page 51).	
3. Set up temporary Release 7.0(x), 7.1(x), or 7.2(x) HDS/Distributor AW.	Before performing a TR upgrade: • Install Windows 2003 and the latest service pack. • Deploy the Windows Firewall scripts. • Install SQL Server 2000, including the latest supported service pack. • Install Release 2.3(1) Support Tools Agent. • Install the required Third Party software. • Install the newly deployed servers. • Verify system conditions using the EDMT. For additional information refer to Setting Up the Hardware (page 35).	
4. Upgrade the Side A HDS/Distributor AW.	Refer to the Distributor AW/HDS Common Ground Upgrade (page 125).	
5. Install the WebView server(s) if not co-located on the AW/HDS.	Refer to the **WebView Installation Guide**[6].	
Start of Central Controller Upgrade Maintenance Window	**********	**********
6. Upgrade the Side A Logger.	Refer to the Logger Common Ground Upgrade: Side A/B (page 135).	
7. Upgrade the Side A CallRouter.	Refer to the CallRouter Common Ground Upgrade: Side A (page 140).	
8. Bring down the side B CallRouter, Logger, and all distributor and client AWs.	None. Refer to the How to Bring Side A into Service (page 141).	

6) http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/report7/index.htm

Step/Completed	Action/Reference	Comments
Bring up the upgraded Side A CallRouter, Logger, and HDS/Distributor AW.		
9. Upgrade the Side B Logger.	Refer to the Logger Common Ground Upgrade: Side A/B (page 135).	
10. Upgrade Side B CallRouter.	Refer to the CallRouter Common Ground Upgrade: Side B (page 143).	
End of Central Controller Upgrade Maintenance Window	**********	**********
11. Upgrade the Side B HDS/Distributor AW and bring it into service once the upgrade is completed. This can begin at any point after step 8.	Refer to the Distributor AW/HDS Common Ground Upgrade (page 125).	
12. Upgrade the AWs, PGs, RMS, and CIS components.	Refer to Administrative Workstation (AW) Upgrade Procedures (page 115). Refer to the Peripheral Gateway (PG) Upgrade Procedures (page 147). Refer to the Remote Monitoring System (RMS) Upgrade Procedures (page 171). Refer to the CIS Upgrade Procedures (page 165).	

Common Ground Upgrade Checklists

Select the appropriate Common Ground checklist for your ICM/IPCC system upgrade.

Table 9: Production HDS/Distributor AW Upgraded in Parallel with the Central Controller Upgrade Maintenance Window

Warning: In order to complete an upgrade successfully, the order of upgrade as defined in this checklist MUST be followed.

Step/Completed	Action/Reference	Comments
1. Upgrade the production system to the required baseline.	Complete the applicable baseline requirements: • Ensure all ICM nodes are at ICM/IPCC Release 7.0(x), ICM/IPCC Release 7.1(x) or ICM/IPCC Release 7.2(x). • Ensure all ICM/IPCC nodes are running Windows 2000 SP4 or Windows 2003.	

Step/Completed	Action/Reference	Comments
	• Ensure the Logger and HDS are running SQL Server 2000 or SQL Server 2005, as appropriate, including the latest supported service pack. • Ensure the CAD is at Release 6.0, 7.0, 7.1, or 7.2 on Windows 2000 Server SP4 or Windows 2000 Advanced Server. • Ensure the CTI OS desktops are at Version 7.0(x), 7.1(x), or 7.2(x). • Ensure CEM, CCS, CMB at Version 6.0, 7.0, or 7.5. • Ensure DCA is at Version 2.1. • Ensure CCM is at Version 4.1, 4.2, 5.0, or 6.0, with the compatible IP IVR or CVP (ISN) version. • Ensure all ACDs are at a version compatible with ICM/IPCC 7.5(1). • Ensure the hardware meets BOM specifications. • Create and configure the Active Directory environment for ICM/IPCC. • Run the Windows firewall configuration scripts to enable network connectivity. • Ensure the ICM/IPCC Support Tools Server is upgraded to Version 2.3(1). • Perform a backup of the existing servers and verify the backups. For additional information refer to Baseline Requirements (page 21).	
2. Create the Active Directory environment.	AD considerations for upgrade: • Migrating users from the old domain to the new domain. • Put the new servers in the Active Directory domain in the appropriate ICM OU. • Validate IP connectivity and remote access. • If the AD domain controller is on the Logger, migrate the domain controller roles to new non-ICM servers. **Note:** Refer to "Migrating Active Directory and DNS to a Non-ICM Server" for additional information.	

Step/Completed	Action/Reference	Comments
	• Bring up the new domain controllers on the domain in which the ICM operates. • Transfer any applicable flexible single master operations (FSMO) roles. • Demote the domain controller on the production Logger to a member server. For additional information refer to Active Directory and DNS Considerations for Upgrades (page 51).	
3. Set up a temporary 7.5(1) HDS/Distributor AW.	Refer to Setting Up a Temporary ICM/IPCC AW/HDS (page 126).	
Start of Central Controller Upgrade Maintenance Window	**********	**********
4. Upgrade the Side A HDS/Distributor AW.	Refer to Distributor AW/HDS Common Ground Upgrade (page 125).	
5. Upgrade the Side A Logger.	Refer to Logger Common Ground Upgrade: Side A/B (page 135).	
6. Upgrade the Side A CallRouter.	Refer to CallRouter Common Ground Upgrade: Side A (page 140).	
7. Install the WebView server(s) if not co-located on the AW/HDS.	Refer to the **WebView Installation Guide**[7].	
8. Bring down the side B CallRouter, Logger, and all distributor and Client AWs. Bring up the upgraded Side A CallRouter and Logger. Point the temporary HDS/Distributor AW to the upgraded Side A CallRouter and Logger.	None. Refer to How to Bring Side A into Service (page 141). None.	
9. Upgrade the Side B CallRouter.	Refer to CallRouter Common Ground Upgrade: Side B (page 143).	
10. Upgrade the Side B Logger.	Refer to Logger Common Ground Upgrade: Side A/B (page 135).	
End of Central Controller Upgrade Maintenance Window	**********	**********
11. Upgrade the Side B HDS/Distributor AW.	Refer to Distributor AW/HDS Common Ground Upgrade (page 125).	

7) http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/report7/index.htm

Step/Completed	Action/Reference	Comments
12. Bring up the Upgraded Side A HDS/Distributor AWs, when available, at any point after Step 8.	None.	
13. Bring up the Upgraded Side B HDS/Distributor AW.	None.	
14. Upgrade the AWs, PGs, RMS, and CIS components.	Refer to Administrative Workstation (AW) Upgrade Procedures (page 115). Refer to Peripheral Gateway (PG) Upgrade Procedures (page 147). Refer to Remote Monitoring System (RMS) Upgrade Procedures (page 171). Refer to CIS Upgrade Procedures (page 165).	

Table 10: Production HDS/Distributor AW Upgraded before the Central Controller Upgrade Maintenance Window

Warning: In order to complete an upgrade successfully, the order of upgrade as defined in this checklist MUST be followed.

Step/Completed	Action/Reference	Comments
1. Upgrade the production system to the required baseline.	Complete the applicable baseline requirements: • Ensure all ICM nodes are at ICM/IPCC Release 7.0(x), ICM/IPCC Release 7.1(x) or ICM/IPCC Release 7.2(x). • Ensure all ICM/IPCC nodes are running Windows 2000 SP4 or Windows 2003. • Ensure the Logger and HDS are running SQL Server 2000 or SQL Server 2005, as appropriate, including the latest supported service pack. • Ensure the CAD is at Release 6.0, 7.0, 7.1, or 7.2 on Windows 2000 Server SP4 or Windows 2000 Advanced Server. • Ensure the CTI OS desktops are at Version 7.0(x), 7.1(x), or 7.2(x). • Ensure CEM, CCS, CMB at Version 6.0, 7.0, or 7.5. • Ensure DCA is at Version 2.1. • Ensure CCM is at Version 4.1, 4.2, 5.0, or 6.0, with the compatible IP IVR or CVP (ISN) version.	

Step/Completed	Action/Reference	Comments
	• Ensure all ACDs are at a version compatible with ICM/IPCC 7.5(1). • Ensure the hardware meets BOM specifications. • Create and configure the Active Directory environment for ICM/IPCC. • Run the Windows firewall configuration scripts to enable network connectivity. • Ensure the ICM/IPCC Support Tools Server is upgraded to Version 2.3(1). • Perform a backup of the existing servers and verify the backups. For additional information refer to Baseline Requirements (page 21).	
2. Create the Active Directory environment.	AD considerations for upgrade: • Migrating users from the old domain to the new domain. • Put the new servers in the Active Directory domain in the appropriate ICM OU. • Validate IP connectivity and remote access. • If the AD domain controller is on the Logger, migrate the domain controller roles to new non-ICM servers. **Note:** Refer to "Migrating Active Directory and DNS to a Non-ICM Server" for additional information. • Bring up the new domain controllers on the domain in which the ICM operates. • Transfer any applicable flexible single master operations (FSMO) roles. • Demote the domain controller on the production Logger to a member server. For additional information refer to Active Directory and DNS Considerations for Upgrades (page 51).	
3. Set up temporary Release 7.0(x), 7.1(x), or 7.2(x) HDS/Distributor AW.	Refer to Setting Up a Temporary ICM/IPCC AW/HDS (page 126).	
4. Upgrade the Side A HDS/Distributor AW.	Refer to Distributor AW/HDS Common Ground Upgrade (page 125).	

Step/Completed	Action/Reference	Comments
5. Install the WebView server(s) if not co-located on the AW/HDS.	Refer to the **WebView Installation Guide**[8].	
Start of Central Controller Upgrade Maintenance Window	**********	**********
6. Upgrade the Side A Logger.	Refer to Logger Common Ground Upgrade: Side A/B (page 135).	
7. Upgrade the Side A CallRouter.	CallRouter Common Ground Upgrade: Side A (page 140)	
8. Bring down the side B CallRouter, Logger, and all distributor and client AWs. Bring up the upgraded Side A CallRouter, Logger, and HDS/Distributor AW.	None. Refer to How to Bring Side A into Service (page 141).	
9. Upgrade the Side B Logger.	Refer to Logger Common Ground Upgrade: Side A/B (page 135).	
10. Upgrade the Side B CallRouter.	Refer to CallRouter Common Ground Upgrade: Side B (page 143).	
End of Central Controller Upgrade Maintenance Window	**********	**********
11. Upgrade the Side B HDS/Distributor AW and bring it into service once the upgrade is completed.	Refer to Distributor AW/HDS Common Ground Upgrade (page 125).	
12. Upgrade the AWs, PGs, RMS, and CIS components.	Refer to Administrative Workstation (AW) Upgrade Procedures (page 115). Refer to Peripheral Gateway (PG) Upgrade Procedures (page 147). Refer to Remote Monitoring System (RMS) Upgrade Procedures (page 171) Refer to CIS Upgrade Procedures (page 165).	

8) http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/report7/index.htm

Part 3: Post-upgrade Testing

Chapter 22

Post-Upgrade Testing

Develop a Test Plan

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/IPCC 7.5(1) 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 (Optional)

Step 1 Open the commonly used WebView views.

Step 2 Examine the data presented.

Internet Script Editor Testing (Optional)

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

Step 2 Examine the data presented.

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 (page 191)).

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.

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/IPCC release 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.

Index