CISCO SYSTEMS

Installation Guide
Cisco ICM/IPCC Enterprise & Hosted Editions
Release 7.1(1)

June 2006

Table of Contents

List of Figures

Preface

Purpose

The Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) provides all information necessary to install ICM/IPCC (including System IPCC) Enterprise & Hosted systems, Release 7.1(1).

Audience

This document is intended for system administrators and engineers responsible for installing this minor release on an existing ICM/IPCC 7.0(0) system.

Organization

This document consists of the following sections:

Section	Description
Chapter 1: Introduction	This chapter provides an overview of ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1).
Chapter 2: Installing ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)	This chapter provides information and the procedures for installing ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1).
Chapter 3: Uninstalling ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)	This chapter provides information and the procedures for permanently or temporarily uninstalling ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1).
Chapter 4: Silent Installation and Manual Recovery from Installer Failures	This chapter provides information and the procedures for running Silent Installations of the ICM 7.1(1) Minor Release Installer. In addition, this chapter informs you how to manually recover from unusual and catastrophic failures of the Installer.

Section	Description
Chapter 5: Upgrading to Cisco CTI OS, Release 7.1(1)	This chapter discusses upgrading CTI OS and refers you to where you can find information dealing with the installation and uninstallation of Cisco CTI OS Release 7.1(1).
Chapter 6: Upgrading to Cisco CAD, Release 7.1(1)	This chapter discusses upgrading CAD and refers you to where you can find information dealing with the installation and uninstallation of Cisco CAD Release 7.1(1).

Related Documentation

- **Cisco CTI OS System Manager's Guide for ICM/IPCC Enterprise & Hosted Edition, Release 7.1(1)** (http://www.cisco.com/en/US/products/sw/custcosw/ps14/ prod_installation_guides_list.html)

- **Cisco CAD Installation Guide, IP Contact Center Enterprise & Hosted Editions, Release 7.1(1)** (http://www.cisco.com/en/US/products/sw/custcosw/ps427/ prod_installation_guides_list.html)

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. • 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*.

Convention	Description
`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>` • File names. Example: `tserver.properties`. • Directory paths. Example: `C:\Program Files\Cisco`
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Field Alerts and Field Notices

Cisco products may be modified or key processes may be determined important. These are announced through use of the Cisco Field Alert and Cisco Field Notice mechanisms. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com.

This tool enables you to create a profile to receive announcements by selecting all products of interest. Log into **www.cisco.com** (http://www.cisco.com) ; then access the tool at **http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en**.

Cisco Product Security Overview

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

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

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.

- Obtain assistance with security incidents that involve Cisco products.

- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

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

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

Reporting Security Problems in Cisco Products

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

- For Emergencies only: security-alert@cisco.com

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

- For Nonemergencies: psirt@cisco.com

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

- 1 877 228-7302

- 1 408 525-6532

Note: We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

- Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

- EMEA: +32 2 704 55 55

- USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

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

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

http://www.cisco.com/discuss/networking

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

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

Chapter 1

Introduction

Overview

Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) is a minor release for ICM/IPCC Enterprise & Hosted Editions, Release 7.0(0) that introduces and caveats.

Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) is available by:

- Downloading **Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)** (http://www.cisco.com/kobayashi/sw-center/telephony/icm/icm-planner.shtml) .

- Ordering Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1).

  Ordering the **Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) Media Kit** (http://www.cisco.com/kobayashi/sw-center/telephony/icm/icm-planner.shtml)

  To order CDs for ICM and IPCC, complete the **Software Upgrade Request Form** (https://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=421&fid=861) .

Baseline Requirements

You can only install Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) on a Release 7.0(0) system (Release 7.0(0), 7.0(0) SR1, 7.0(0) SR2, and 7.0(0) SR3). If you are running any release previous to Release 7.0(0), all components you want to install Release 7.1(1) on must first be upgraded to a Release 7.0(0) system. In addition, these components must meet the requirements of the **Cisco ICM/IPCC Enterprise & Hosted Editions Hardware and System Software Specifications (Bill of Materials)** (http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm) for these releases.

Release Strategy

Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) is a *minor release*. New as of Release 7.1(1), a minor release is an incremental set of software fixes and a limited set of new functionality delivered in an automated installer.

A minor release is incremental, cumulative to the base release of the Major release, and it can be returned to its pre-installation state. All published maintenance release content present at the point of the minor release ship date is contained within the minor release. The only exception is where a minor release development/testing schedule overlaps with that of a maintenance release. Engineering specials released prior to the code freeze date are also part of the minor release content.

Minor Release 7.1(1) can be installed over ICM/IPCC 7.0(0), or ICM/IPCC 7.0(0) SR1-SR3. The Release 7.1(1) Installer performs a check that prevents it from installing on systems running ICM/IPCC 7.0(0) with service releases after SR3. Subsequent ICM/IPCC 7.1(*x*) maintenance releases will support ICM/IPCC 7.1 installation over ICM/IPCC 7.0(0) service releases after SR3.

For additional information on the Cisco software support methodology, refer to: **Cisco Software Support Release Methodology for Cisco Unified ICM and Cisco Unified Contact Center Enterprise and Hosted Editions** (http://www.cisco.com/kobayashi/sw-center/telephony/icm/icm-planner.shtml).

For an explanation of the specifications for a full ICM/IPCC Enterprise & Hosted Editions, Release 7.0(0) upgrade, refer to the **Cisco ICM/IPCC Enterprise & Hosted Editions Hardware and System Software Specifications (Bill of Materials)** (http://www.cisco.com/univercd/cc/td/doc/product/icm/ccbubom/index.htm) for that release.

New Feature Overview

The Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) new features are installed automatically when the Installer is run.

System IPCC, component roles are somewhat different from ICM component roles. In System IPCC:

- ICM/IPCC Distributor AWs with WebView and HDS have the role of *Administration & WebView Reporting*.

- An IPCC System PG plus CTI Server and CTI OS Server, has the role of *Agent/IVR Controller*.

- The Outbound Option MR PG and Dialer have the role of *Outbound Controller* .

- The Logger and CallRouter are always co-located on the same Central Controller machine.

The new features introduced in Release 7.1(1) include:

- Cisco Unified Mobile Agent

- Persistence Configuration for Expanded Call Context (ECC) Variables

- Support Tools Node Agent is automatically installed. When the Release 7.1(1) Installer is invoked, it in turn invokes the Support Tools Node Agent installer in a silent mode, causing the Node Agent to be installed on ICM/IPCC systems. However, the Support Tool Node Agent process is installed disabled, due to security concerns. To enable the node agent process, refer to the **Security Best Practices Guide for Cisco ICM/IPCC Enterprise & HostedEditions, Release 7.0(0)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html) to learn how to enable IPSEC filtering between the Support Tools Node Agent and the Support Tools Server.

- With Release 7.1(1), the Contact Center SNMP Management service enables the Contact Center SNMP infrastructure if CRS 4.0(2) or greater is installed, thus replacing Windows SNMP and providing instrumentation of both the CRS and ICM PG components. This change applies to both installation and startup of the Contact Center SNMP Management service.

- JDK and JRE are updated to JDK1.4.2_10 and JRE 1.4.2_10 on:

  - Distributor AW systems with CMS and/or the Agent Re-skilling Web Tool enabled

  - WebView systems

  - CallManager PG systems

  - IPCC System PG systems

- Support for the InstallShield Silent Installation

  InstallShield Silent Install (also known as silent installation) allows you to automate your electronic software distribution. Using *InstallShield Silent*, there is no need for you to monitor the installation and provide input by completing dialog boxes. An *InstallShield Silent* installation runs on its own, without any intervention on your part. For additional information, refer to Silent Installations (page 41).

- The prior System IPCC language restriction is lifted and there is now installation support for full local language selection. All languages available to the ICM are now available on System IPCC platforms.

- CAD enhancement including CAD Browser Edition (BE), CAD IP Phone Agent, Supervisor Desktop, Server, and accessibility enhancements.

  Note: Installed using the CAD Release 7.1(1) Installer.

- CTI OS support for Citrix and Silent Monitor

  Note: Installed using the CTI OS Release 7.1(1) Installer.

For more detailed information concerning the Release 7.1(1) new features, refer to the **Release Notes for Cisco IPCC/ICM Enterprise & Hosted Editions, Release 7.1(1)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_release_notes_list.html)

About the Release 7.1(1) Installer

Release 7.1(1) Installer

As there are various ICM system configurations, ensure you have the appropriate installers for your combination of Release 7.1(1) core component software (ICM/IPCC Enterprise, ICM/IPCC Hosted, System IPCC) and desktop software (CTI OS Server, CTI OS Client, CAD) to match your specific system.

When launched, the new Release 7.1(1) Installer performs actions such as stopping services, file installations, the schema upgrade, and any necessary registry modifications. The Installer also automatically determines if the basic requirements are met to allow the installation to continue. If a requirement is not met, the Installer corrects the problem if it can; otherwise it displays instructions so you can manually correct the problem, then it exits. As well as displaying the error on the screen, each component logs the error to their respective log file.

Note: System IPCC component roles are somewhat different from ICM/IPCC component roles. ICM/IPCC Distributor AWs with WebView and HDS have the role of *Administration & WebView Reporting* in System IPCC. An IPCC System PG plus CTI Server and CTI OS Server in System IPCC has the role of *Agent/IVR Controller*. The Outbound Option MR PG and Dialer have the role of *Outbound Controller*. In System IPCC, the Logger and CallRouter are always co-located on the same Central Controller machine.

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

Note:

- Ensure you have run the Release 7.1(1) Installer on all your remaining AWs before bringing them online.

- The Peripheral Gateways do not necessarily have to be upgraded during the same maintenance window as the Central Controllers.

The Installer also performs uninstallation. You can perform either a *Permanent* uninstallation or a *Temporary* uninstallation.

Note: The option to perform a temporary uninstallation is only available on components having a database (the Loggers, HDSs, and Distributor AWs). Components not having a database can only be permanently uninstalled.

Permanent Uninstallation

Selecting a *Permanent* uninstallation performs both a rollback of the database schema to the Release 7.0(0) schema and uninstalls the Release 7.1(1) application; deleting all configuration data specific to Release 7.1(1). New or changed configuration data that is unrelated to Release 7.1(1) features (for example, new agents and skill groups) is, however, retained.

A permanent uninstallation performs the following tasks:

• Performs the uninstallation of the Release 7.1(1) application.

• Reverts the database to the ICM/IPCC 7.0(0) schema version.

• Logs the results, then exits.

Temporary Uninstallation

Selecting a *Temporary* uninstallation uninstalls the Release 7.1(1) application, but does not perform a database rollback.

Note: If you choose the *Temporary* option, the Logger, AW, and HDS components can not come online until Release 7.1(1) is reapplied. If you try to bring them online without reinstalling Release 7.1(1), an error is displayed indicating that there is a schema version mismatch.

The following are not uninstalled when either a *Temporary* uninstallation or a *Permanent* uninstallation is performed:

• the JRE/JDK version

• Support Tools

Release 7.1(1) Installation/Uninstallation Overviews

The following sections provide an overview of an installation and an uninstallation of Cisco ICM/IPCC Enterprise & Hosted Edition, Release 7.1(1).

High Level Overview of a Release 7.1(1) Installation

1. Bring the system to the baseline (page 11).

2. Perform a backup of both the side A and side B Logger and the HDS (Administration & WebView Reporting) databases using Microsoft SQL Server Enterprise Manager.

3. Disable configuration changes on both the side A and the side B Central Controllers.

   How to 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 installed.

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.

4. Perform a backup of the configuration data from one of the sides using ICMDBA.

How to back up the Configuration Database using ICMDBA

– Create a directory on a local drive. Ensure that the drive has enough available disk space to support the backup of your configuration database.

Note: Configuration databases can vary drastically in size from one customer to another. The size ranges from a small configuration of about 15 MB to 150 MB on the larger side. If you are about to back up your configuration for the first time, and you are uncertain of the size of your configuration, plan for at least double the amount of the higher number on the drive where you want to store the backup. For example, plan for about 300 MB.

– Using Windows Explorer, navigate to the icm\bin directory to locate the ICMDBA executable. By default, the icm\bin directory resides on the system drive. The full path for the executable is <*ICM installed drive*>:\icm\bin.

– Double-click **ICMDBA.exe**, the ICMDBA application window appears.

– Expand **Instances** to locate your Customer Instance.

– Drill down under your Customer Instance to the database.

– Select **Data > Export** from the menu bar. The Export data from window appears.

The default value in the Data type field is **Configuration**. The default Destination Path is **c:**.

– Click **Browse** to navigate to the directory you created in Step 1.

– Click **Export** when you are ready to begin the backup.

– Click **Start** in the application window. The export begins. An export completion message appears after successful export of data.

– Click **OK**, and exit ICMDBA.

Note: To verify the successful backup of the configuration data, open a Windows Explorer session. Navigate to the directory you created and verify whether the data

files exist. The amount of space that the combined files take up on your hard disk must accurately reflect the size of your ICM configuration.

Note: While you can start the installation on either side A or side B of a duplexed system, for the purposes of this document, it is assumed that side A is the first side to be installed.

5. Stop all side A Central Controller (CallRouter and Logger) services.

6. Run the Release 7.1(1) Installer on the side A Central Controller.

7. Stop the services of the primary Distributor AW/HDS (Administration & WebView Reporting) associated with the side A Cental Controller.

8. Run the Release 7.1(1) Installer on that primary Distributor AW/HDS (Administration & WebView Reporting).

9. To complete the installation process, reboot the side A Central Controller and the primary Distributor AW/HDS (Administration & WebView Reporting) associated with the side A Cental Controller.

10. Stop all side B Central Controller (CallRouter and Logger) services. This causes default routing to occur.

11. Start the side A Central Controller and the primary Distributor AW/HDS (Administration & WebView Reporting) services associated with the side A Cental Controller.

12. Verify side A operation.

    Note: If side A is not operating properly, stop all side A services, return side B to service, and perform an uninstallation on side A. Resolve any issues encountered, then restart the installation process.

13. Run the Release 7.1(1) Installer on the side B Central Controller.

14. Stop the services of the primary Distributor AW/HDS (Administration & WebView Reporting) associated with the side B Cental Controller.

15. Run the Release 7.1(1) Installer on that primary Distributor AW/HDS (Administration & WebView Reporting).

16. To complete the installation process, reboot the side B Central Controller and the primary Distributor AW/HDS (Administration & WebView Reporting) associated with the side B Cental Controller.

17. Start the side B Central Controller and Distributor AW/HDS (Administration & WebView Reporting) services associated with the side B Cental Controller.

18. Enable configuration changes on both the side A Central Controller and the side B Central Controller.

    How to enable configuration changes:

– 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 installed.

Note: RouterA in the registry key above is RouterB on the Side B CallRouter.

– Verify that configuration changes are possible.

19. Verify side B operation.

20. **Note:** The PG and CTI OS components must be upgraded to Release 7.1(1) in the same maintenance window. Running them mixed is not supported.

Perform the following:

– **Note:** Perform this action first.

Stop the PG and CTI OS Server (Agent/IVR Controller) services and install ICM/IPCC Release 7.1(1) and CTI OS Release 7.1(1) on the PGs and CTI OS Servers (Agent/IVR Controllers), respectively.

Note: The remaining actions can be performed in any order.

– Stop all remaining Distributor AW/HDS (Administration & WebView Reporting) and Client AW services and install Release 7.1(1) on the remaining Distributor AW/HDSs and Client AWs.

– Stop the CTI OS Desktop services and install CTI OS Release 7.1(1) on the CTI OS Desktops.

Note: Agent/Supervisor Desktops need not be upgraded to 7.1(1) in the same maintenance window as the PG and CTI OS servers.

– Stop the CAD Desktop services and install CAD Release 7.1(1) on the CAD desktops.

21. After the installation process has completed, and both the A and B sides of your system are operating properly, set the ICM/IPCC services that were changed from their original setting of **Automatic** to **Manual** for the installation, back to **Automatic** to ensure that the system functions properly after a reboot.

Note: If you are not sure which services were changed from **Automatic** to **Manual** during the installation of the Release 7.1(1), examine the setup logs located in C:\Temp\Minor Release ICM 7.1(1).

High Level Overview of a Release 7.1(1) Permanent Uninstallation

1. Disable configuration changes on both the side A and the side B Central Controllers.

How to 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 installed.

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. Perform the following:

– **Note:** Perform this action first.

Stop the PG and CTI OS Server (Agent/IVR Controller) services and uninstall CTI OS Release 7.1(1) on the PGs and CTI OS (Agent/IVR Controller) Servers.

Note: The remaining actions can be performed in any order.

– Stop the CTI OS Desktop services and uninstall CTI OS Release 7.1(1) on the CTI OS desktops.

– Stop the CAD Desktop services and uninstall CAD Release 7.1(1) on the CAD desktops.

– Stop all remaining Distributor AW/HDS (Administration & Webview Reporting) and Client AW services and uninstall Release 7.1(1) from the remaining Distributor AW/HDSs (Administration & WebView Reporting) and Client AWs.

3. Stop the services on a Distributor AW/HDS (Administration & WebView Reporting) associated with the side A Cental Controller.

4. Uninstall the Distributor AW/HDS (Administration & WebView Reporting) associated with the side A Cental Controller using the Release 7.1(1) Installer.

5. Stop all side A Central Controller (CallRouter and Logger) services.

6. Uninstall the side A Central Controller using the Release 7.1(1) Installer.

7. After the uninstallation process has completed, reboot the side A Central Controller and the Distributor AW/HDS (Administration & WebView Reporting) associated with the side A Cental Controller.

8. Stop all side B Central Controller (CallRouter and Logger) services. This causes default routing to occur.

9. Start the side A Central Controller and Distributor AW/HDS (Administration & WebView Reporting) services associated with the side A Cental Controller.

10. Verify side A operation and bring side A into service.

11. Stop the services on a side B Distributor AW/HDS (Administration & WebView Reporting) associated with the side B Cental Controller.

12. Uninstall the Distributor AW/HDS (Administration & WebView Reporting) associated with the side B Cental Controller using the Release 7.1(1) Installer.

13. Uninstall the side B Central Controller using the Release 7.1(1) Installer.

14. After the uninstallation process has completed, reboot the side B Central Controller and the Distributor AW/HDS (Administration & WebView Reporting) associated with the side B Cental Controller.

15. Start the side B Central Controller and the Distributor AW/HDS (Administration & WebView Reporting) associated with the side B Cental Controller services.

16. Verify side B operation and bring side B into service.

17. Stop all remaining Distributor AW/HDS (Administration & WebView Reporting) and Client AW services and uninstall Release 7.1(1) on the remaining Distributor AW/HDSs and Client AWs.

18. Upon completion of the uninstallation reboot and verify the operation of all remaining Distributor AW/HDS (Administration & WebView Reporting) and Client AW services.

19. Enable configuration changes on both the side A Central Controller and the side B Central Controller.

How to enable configuration changes:

- 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 installed.

  Note: RouterA in the registry key above is RouterB on the Side B CallRouter.

- Verify that configuration changes are possible.

20. After the uninstallation process has completed, and both the A and B sides of your system are operating properly, set the ICM/IPCC services that were changed from their original setting of **Automatic** to **Manual** for the uninstallation back to **Automatic** to ensure that the system functions properly after a reboot.

    Note: If you are not sure which services were changed from **Automatic** to **Manual** during the uninstallation of the Release 7.1(1), examine the setup logs located in C:\Temp\Minor Release ICM 7.1(1).

Local Setup versus Media Setup

ICM Setup behaves differently when installed from the release media than it does running from the icm\bin directory. Running *setup.exe* from the media is referred to as *Media Setup*.

Running *ICMsetup.exe* from the icm\bin directory is referred to as *Local Setup*

Note: There is no concept of *Local Setup* for System IPCC. The applicable tasks performed by *Local Setup* are performed in System IPCC by the *Web Administration Tool*.

The Release 7.1(1) media can only be used to install or uninstall Release 7.1(1). The 7.0(0) *Media Setup* is used to install new ICM components. You cannot run Release 7.0(0) *Media Setup* on a system having Release 7.1(1) already installed.

Note: If a CallRouter, Logger, AW, or WebView Server was not previously installed on a Release 7.1(1) system, these components can only be installed using Release 7.0(0) *Media Setup* after you have uninstalled all Release 7.0(0) and Release 7.1(1) service/maintenance releases. If the CallRouter, Logger, AW, or WebView Server components previously existed, a new CallRouter, Logger, AW, or WebView Server instance can be installed using *Local Setup*.

Local Setup Changes

Running *Local Setup* after applying Release 7.1(1) to an ICM 7.0(0) base system allows you to:

- Add new instances (even not previously installed).

- Add new components (even not previously installed) such as:

  - PG

- Outbound Option Dialer

- MEI Server

- Inap Gateway

- Application Bridge Server

- CTI Server

- CompuCall Gateway Server

- Change the PIM type for any PG selected

- Run *Local Setup* on an AW Distributor to enable:

  - CMS

  - Agent Reskilling WebTool

  - Internet Script Editor

  - WebView Database

You can add the above components without the need to uninstall the minor or maintenance/service releases.

ICM Setup Rollback Support

The uninstallation of Release 7.1(1) enables a return to the previous state. For example, if the Release 7.1(1) version is applied on a system that had ICM 7.0 SR2 applied, the uninstallation of the Release 7.1(1) restores the system to the ICM 7.0 SR2 state.

The most important Release 7.1(1) change is the creation of new services that depend on files added, or modified, by the Installer. *Local Setup* records the data for these services to be used by the Installer's uninstallation process to safely disable or remove these services if necessary.

If you choose to perform a temporary uninstallation of Release 7.1(1), the services are only disabled.

When Release 7.1(1) is reapplied:

- All services set to **Automatic** are changed to **Manual**.

- All new feature services disabled when the uninstallation was performed are re-enabled. Any services disabled prior to the uninstallation remain disabled.

If you perform a permanent uninstallation of Release 7.1(1) and you want all references to the components cleaned from the system, the proper approach is to delete the component for that instance. To delete a component, select it from the Instance Components list, and click **Delete**.

Retasking a Machine

While any machine can be retasked, normally you will be retasking an AW Distributor as a WebView server. This can only be accomplished by running Setup from the Release 7.0(0) media.

After Release 7.1(1) is applied, the only way a WebView server can be added to the Distributor system as a new component is by uninstalling Release 7.1(1) and all the Release 7.0 service releases up to the Release 7.0 base. You can then add the WebView server using the Release 7.0 *Media Setup*. Once the WebView server has been added, reapply Release 7.1(1).

In general, after Release 7.1(1) has been applied, the only way a new component (Logger, CallRouter, AW, or WebView) can be added to any ICM/IPCC system as a new component is by uninstalling Release 7.1(1) and all the Release 7.0 service releases up to the Release 7.0 base. You can then add the new component using the Release 7.0 *Media Setup*. Once the new component has been added, reapply Release 7.1(1).

Note: There is no need to reapply the 7.0 service releases as you can reapply Release 7.1(1) directly on top of Release 7.0(0). See the Release Strategy (page 12) section for additional information.

In general, the **Cisco ICM/IPCC Enterprise & Hosted Editions Hardware and System Software Specifications (Bill of Materials).** (http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm) for this release recommends each ICM component be installed on a separate box.

Note: In System IPCC, retasking a machine is accomplished using the *Web Administration Tool* by changing, within defined limits, the role of the machine.

Schema Deployment Overview

When you invoke the Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) Installer, it makes additions and/or modifications to the database schema. These schema modifications do not require your intervention at the time of installation.

For more detailed information concerning schema changes for Release 7.1(1), refer to the **Release Notes for Cisco IPCC/ICM Enterprise & Hosted Editions Release 7.1(1)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_release_notes_list.html)

For more detailed information concerning the Release 7.0(0) schema, refer to the **Database Schema Handbook for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.0(0)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html)

For more detailed information concerning the Release 7.1(1) schema, refer to the **Database Schema Handbook, Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html)

New Log Files

<hostname>_<instancename>_<databasename>.log

A new log file is introduced during the Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) installation and uninstallation. This log is located in the *<install drive>*:\temp directory and contains the database related results of the installation and uninstallation processes.

The *<hostnameinstancenamedatabasename>*.log file contains the following information:

- SR Version of the *installation* and the *return* executables writing to this file:

  – ICM/IPCC 7.1(1)

- DB modification type:

  – SR Database Installation

  – SR Database Return

- ICM/IPCC version and schema version the executable has at the start:

  – ICM/IPCC 7.0(0), Schema version 95

  – ICM/IPCC 7.1(1), Schema version 96

- ICM/IPCC version and schema version the executable has upon completion:

  – ICM/IPCC 7.0(0), Schema version 95

  – ICM/IPCC 7.1(1), Schema version 96

- Status message:

  – Success:

    Indicates upgrade completed successfully and provides the current database version.

  – Failure:

    Indicates upgrade failed and provides error messages.

<date>_<time>_Minor Release ICM7.1(1).log

This is a date stamped log file created each time an installation or an uninstallation is performed, logging information concerning that specific installation or uninstallation.

The naming convention for these separate non-concatenated logs is **<date>_<time>_Minor Release ICM7.1(1).log**, and they are created in the **<Install Drive>:\temp\Minor Release ICM7.1(1)** directory.

Overview

Chapter 2

Installing ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) Core Components

Prior to installing ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) core components, ensure you have met both the baseline requirements (page 11) and the requirements of the **Cisco ICM/IPCC Enterprise & Hosted Editions Hardware and System Software Specifications (Bill of Materials)** (http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm) for this release.

In addition, review the **Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) Release Notes** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/ prod_release_notes_list.html) and the High Level Overview of a Release 7.1(1) Installation (page 15) section.

Ensure you take the following into consideration when installing Release 7.1(1):

- A minimum of 1.2 GB of disk space is needed on the disk drive on which the ICM is installed.

- JDK/JRE versions 1.5 or later are not supported and must be uninstalled prior to installing Release 7.1(1).

- All CallRouter, Logger, AW, and WebView systems must have Release 7.1(1) installed prior to bringing up the services.

The installation process performs the following tasks and logs the results of each step performed:

- Checks the SQL Server Master database for the existence of any ICM/IPCC database

- Checks the database version

  - If the version is the ICM/IPCC 7.0(0) schema version, the Installer checks if the new table(s) and/or column(s) exist. If they do, it drops the table(s), logs the results, and exits.

    If the new table(s) and/or column(s) do not exist, the Installer performs the installation, logs the results, and then exits.

- If the version is the ICM/IPCC 7.1(1) schema version, the Installer checks if the new table(s) and/or column(s) exist. If they do, it logs the results and exits.

  If the new table(s) and/or column(s) do not exist, the Installer performs the installation, logs the results, and then exits.

  Note: This case is very unlikely, however, it ensures that if the schema version equals the ICM/IPCC 7.1(1) schema version, but the schema itself does not reflect the ICM/IPCC 7.1(1) schema version, the schema changes are made and the event logged.

How to install ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) Core Components

Perform the following steps to install ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) core components:

Step 1   Log onto your system as a user with administrative privileges.

Step 2   After either downloading the Installer or placing the media in the drive, start the **ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) Installer**.

The InstallShield Wizard opens, briefly displays the Preparing Setup dialog box.

During the next few moments the Installer determines:

- if you (the logged on user) have local administrative rights.

  - If you do have administrative rights, the installation continues.

  - If you do not have administrative rights, the Installer posts an error message with instructions, then exits.

- if the correct ICM product/version is installed.

  - If the correct product/version is installed, the installation continues.

  - If the correct product/version is not installed, the Installer posts an error message with instructions, then exits.

- the service release level, if any, the product has installed.

- if Cisco Security Agent (CSA) is installed. The Installer then determines the CSA version and if the service is running.

  The CSA check indicates that one of the following set of conditions exists:

  - If the correct version of the CSA service (4.5 or later) is up and running, the Installer requests permission from you to stop the CSA service. If you select **Yes**, a warning message is displayed.

    If you do not want the Installer to stop the service, select **No**, the Installer exits.

If you select **Yes**, the Installer stops the service and displays a status message.

Note: If the confirmation dialog is not displayed when attempting to stop the CSA service on a machine that has had users logged into it using a session of Remote Desktop Connection, the CSA service can not be stopped. The Installer hangs while displaying the "Stopping CSA" dialog. Use the Windows Task Manager to disconnect and logoff any users that are currently, or have previously been, connected to the system. Before attempting to stop CSA again, either allow the initial request to stop CSA to timeout, or reboot the system.

– If the service is running but the CSA version is not 4.5 or later, the Installer displays an error message, then exits.

– If the service is not running, and the CSA version is not 4.5 or later, the Installer displays a warning message, then provides the option to continue or not:

If you select **No**, the Installer exits.

If you select **Yes**, the installation continues.

The Welcome to the InstallShield Wizard dialog box appears.

Step 3 Click **Next**.

The License Agreement dialog box appears.

Step 4 Select **I accept the terms of the license agreement**, then click **Next**.

If you do not accept the license agreement, an error screen is displayed and the Installer exits.

The Select Language dialog box appears.

Note: Prior to making your language selection, refer to the **Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) Release Notes** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_release_notes_list.html) for this release for information concerning language version selection.

Figure 1: Select Language Dialog Box
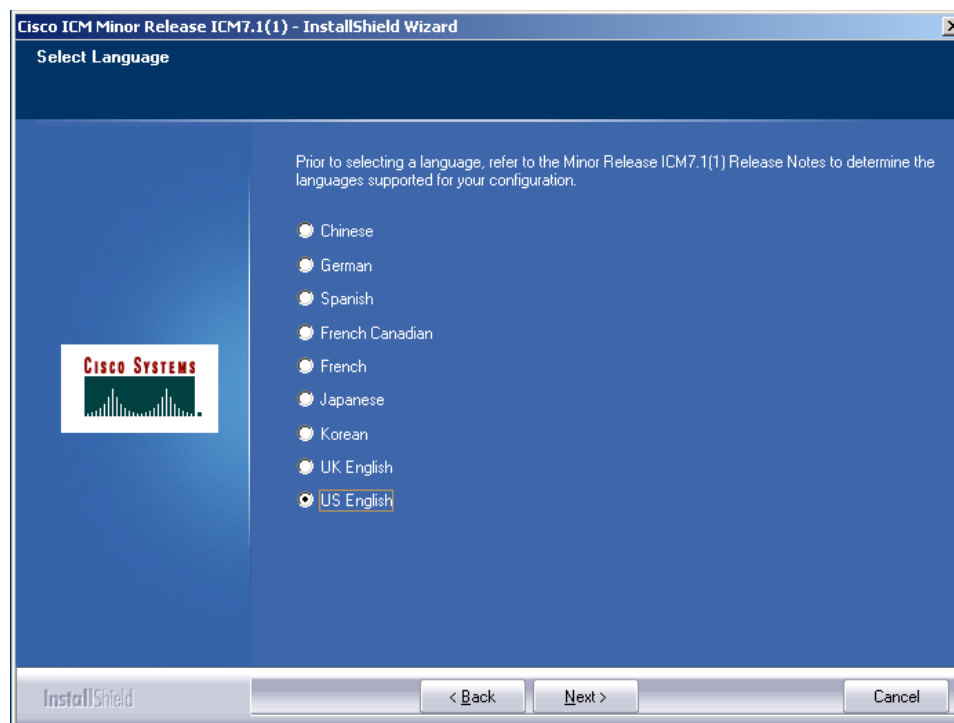
Step 5   Select the appropriate language, then click **Next**.

The Installer now determines if known features were previously installed.

The Ready to Install the Program dialog box is displayed.

Step 6   Click **Install** to start the installation process.

The Setup Status dialog box appears and indicates the progress of the installation. In addition to the status bar, popups appear describing the actions of the Installer (for example, messages indicating when services are being stopped by the Installer).

Note: Shutting down services may take a while. This is normal behavior.

If an error occurs during the installation process, an Installation Errors dialog box appears providing error information. Once you have read the errors, click **Next** and follow the on-screen instructions.

When the installation is complete, the CSA services are restarted, and the InstallShield Wizard Complete dialog box appears.

Step 7   Ensure **Yes, I want to restart my computer now** is selected (the default), then click **Finish**.

After the installation process has completed, and both the A and B sides of your system are operating properly, set the ICM/IPCC services that were changed from their original setting of **Automatic** to **Manual** for the installation back to **Automatic** to ensure that the system functions properly after a reboot.

Note: If you are not sure which services were changed from **Automatic** to **Manual** during the installation of the Release 7.1(1), examine the Messages dialog box that appears at the end of the uninstallation. You can also check the ICM Service Control.

Figure 2: Messages Dialog Box
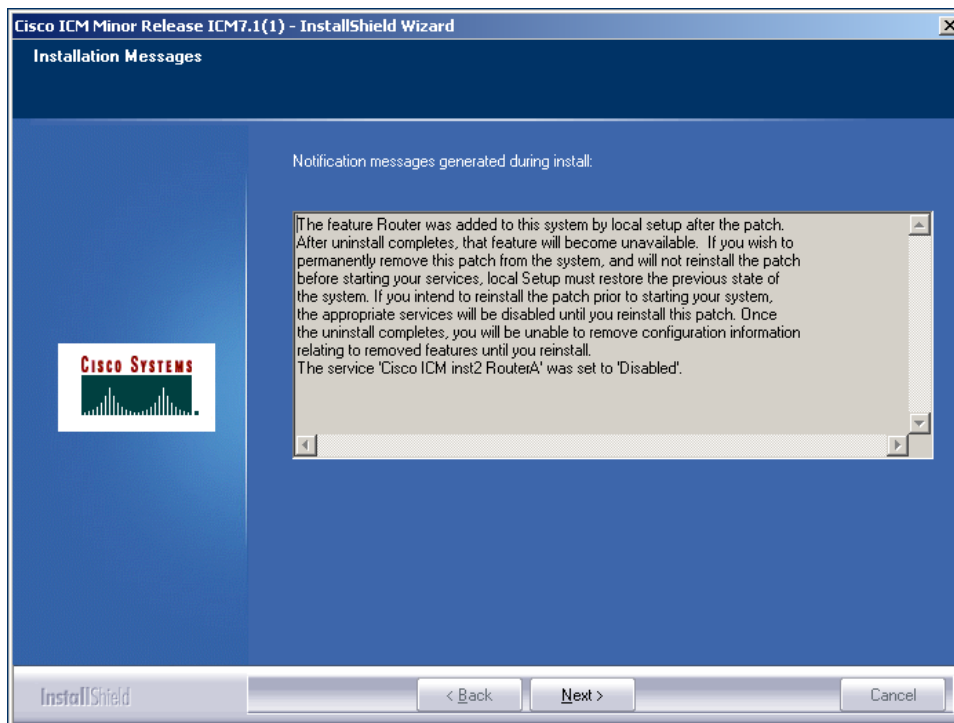
Note: In release 7.1(1), the amount of disk space used by IPCC Enterprise Call Manager PGs and IPCC System PGs is increased (from approximately 300 MB) to approximately 1 GB. The increased disk space usage improves turn around times on sustaining activities. For production systems that follow the hardware guidelines in the ICM/IPCC Enterprise and Hosted Editions Hardware and System Software Specifications (Bill of Materials), Release 7.0(0) / 7.1(1) , this increased disk space usage will not present issues. However, in a laboratory environment there is the possibility that if the lab system is undersized, or if a progger (a PG or Agent/IVR Controller or Outbound Controller; and the CallRouter and Logger or Central Controller; installed on a single machine) allocates too much space for the database, or if in a multi-instance PG/hosted environment several PGs are installed, the amount of disk space required must be considered. Assume that each Call Manager PG on your platform will consume approximately 1.25 GB of disk space for trace logging. If necessary, you can modify the EMSAllLogFilesMax retention setting appropriately for the available disk space on the system.

Chapter 3

Uninstalling ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) Core Components

In the event a problem occurs, you have the ability to uninstall the changes to the database schema that occurred during the installation of Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1). At the time of the uninstallion, you must decide if you wish to "return" the database schema to the previous schema version (a permanent uninstallation) or to leave the schema unmodified (a temporary uninstallation).

Note: Uninstallation procedures are not supported to run silently.

There are two reasons to uninstall a Cisco ICM/IPCC, Release 7.1(1):

- To temporarily uninstall (page 34) the release in order to allow you to install another component from the base 7.0(0) media.

  Note: It is never necessary to perform a temporary uninstallation on a System IPCC system as there is no concept of adding components later from the base media.

- To permanently uninstall (page 36) both the application and the database schema changes; returning the system to the previous service release level and returning the database to the ICM/IPCC 7.0(0) schema version.

  This is necessary if there is a catastrophic failure of a major component in the release and requires the schema changes be returned to the previous schema level.

This section contains the following topics:

Temporarily Uninstalling ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) Core Components

A temporary uninstallation can be performed on any ICM/IPCC system and are performed when Hosted Editions, Release 7.1(1) is reapplied.

Note: A temporary uninstallation is never necessary on a System IPCC deployment. System IPCC does not require adding components using the base media.

The components requiring a temporary uninstallation of Release 7.1(1) to install are the:

- Logger (if installing on an AW)

- CallRouter (if installing on an AW or Logger)

- AW (if installing on a Logger)

- WebView (if installing on an AW or Logger)

Note: The Logger, AW, and HDS components check the version table in the ICM database schema for their corresponding schema version. In the event the schema version and the executable version do not match, a mis-match error message is produced and the services shut down. This error is captured in the component logs.

How to Temporarily Uninstall Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)

Use the Windows Add/Remove Programs utility to uninstall Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1).

To perform a temporary uninstallation:

Step 1   Log onto your system as a user with administrative privileges.

Step 2   Select **Start > Settings > Control Panel**.

The Control Panel dialog box appears.

Step 3   Select **Add or Remove Programs** and then double-click.

The Add or Remove Programs dialog box appears.

Step 4   Select the **Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)** entry.

Step 5   Click **Change/Remove**, then proceed as directed by the Installer.

The InstallShield Wizard opens, briefly displays the Preparing Setup dialog box, then, if running on a machine with a database, displays the Database Schema Rollback dialog box. If not running on a machine with a database, the Setup Status dialog box appears.

During the next few moments, the Installer determines if:

- you (the logged on user) have local administrative rights.

  – If you have administrative rights, the installation continues.

  – If you do not have administrative rights, the Installer posts an error message with instructions, then exits.

- Cisco Security Agent (CSA) is installed. The Installer then determines the CSA version and if the service is running.

  The CSA check indicates that one of the following set of conditions exists:

  – If the correct version of the CSA service (4.5 or later) is up and running, the Installer requests permission from you to stop the CSA service. If you select **Yes**, the following message is displayed and the installation continues.

Warning: Cisco Security Agent Service will be stopped before the Patch installation continues. It will be re-started as soon as the Patch Installation completes. Do you want to Continue?"

  If you do not want the Installer to stop the service, select **No**, the Installer exits.

  If you select **Yes**, the Installer stops the service and displays a status message.

  Note: If the confirmation dialog is not displayed when attempting to stop the CSA service on a machine that has had users logged into it via a session of Remote Desktop Connection, the CSA service can not be stopped. The Installer hangs while displaying the "Stopping CSA" dialog. Use the Windows Task Manager to disconnect and logoff any users that are currently, or have previously been, connected to the system. Before attempting to stop CSA again, either allow the initial request to stop CSA to timeout, or reboot the system.

  – If the service is running but the CSA version is not 4.5 or later, the Installer displays an error message, then exits.

  – If the service is not running, and the CSA version is not 4.5 or later, the Installer displays a warning message, then provides the option to continue or not:

  If you select **No**, the Installer exits.

  If you select **Yes**, the installation continues.

- features were added after the installation.

  If so, warnings and instructions are posted indicating the required action(s).

Figure 3: Database Schema Rollback Dialog Box
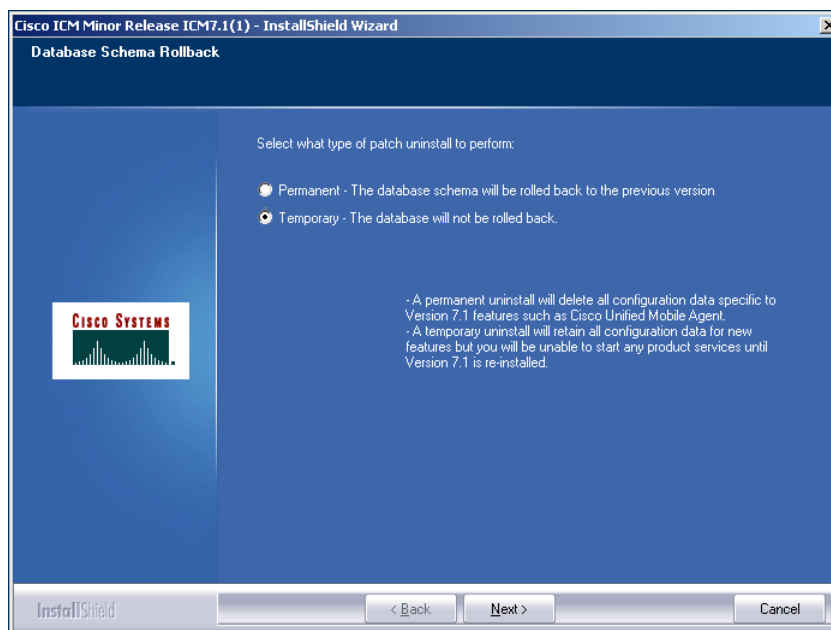
Step 6 Select **Temporary - The database will not be rolled back**, then click **Next**.

A confirmation dialog box appears.

Step 7 Click **Yes**.

The Setup Status dialog box appears and indicates the progress of the temporary uninstallation.

Additional messages may appear as the temporary uninstallation proceeds.

Note: If an error occurs during the temporary uninstallation process, an Uninstallation Errors dialog box appears providing error information. Once you have read the errors, click **Next** and follow the on-screen instructions.

When the temporary uninstallation finishes, the Uninstall Complete dialog box appears.

Step 8 Ensure **Yes, I want to restart my computer now** is selected (the default), then click **Finish**. After the reboot, the temporary uninstallation is complete.

Permanently Uninstalling ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) Core Components

A permanent uninstallation is necessary if there is a catastrophic failure of a major component in the release that requires the schema changes be returned to the previous schema level. This deletes all configuration data specific to Release 7.1(1) features (for example, mobile agent information).

A permanent uninstallation performs the following tasks and logs the results of each step performed:

- Checks the database version

  – Performs the uninstallation of the Release 7.1(1) application, reverts the schema version to the ICM/IPCC 7.0(0) schema version, logs the results, and then exits.

  – If the version is the ICM/IPCC 7.0(0) schema, the Installer logs the results, reports an error, and exits.

Warning: Prior to performing a permanent uninstallation, perform a backup of all databases on the system.

How to Permanently Uninstall Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1)

Use the Windows Add/Remove Programs utility to permanently uninstall the Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1).

To perform a permanent uninstallation:

Step 1   Log onto your system as a user with administrative privileges.

Step 2   Select **Start > Settings > Control Panel**.

The *Control Panel* dialog box appears.

Step 3   Select **Add or Remove Programs** and then double-click.

The *Add or Remove Programs* dialog box appears.

Step 4   Select the Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.1(1) entry.

Step 5   Click **Change/Remove**.

Step 6   Proceed as directed by the Installer.

The InstallShield Wizard opens briefly displaying the Preparing Setup dialog box, then, if running on a machine with a database, displays the Database Schema Rollback dialog box. If not running on a machine with a database, the Setup Status dialog box appears.

During the next few moments, the Installer determines:

- if you (the logged on user) have local administrative rights.

  – If you have administrative rights, the installation continues.

– If you do not have administrative rights, the Installer posts an error message with instructions, then exits.

• if Cisco Security Agent (CSA) is installed. The Installer then determines the CSA version and if the service is running.

The CSA check indicates that one of the following set of conditions exists:

– If the correct version of the CSA service (4.5 or later) is up and running, the Installer requests permission from you to stop the CSA service. If you select **Yes**, the following message is displayed and the installation continues.

Warning: Cisco Security Agent Service will be stopped before the Patch installation continues. It will be re-started as soon as the Patch Installation completes. Do you want to Continue?"

If you do not want the Installer to stop the service, select **No**, the Installer exits.

If you select **Yes**, the Installer stops the service and displays a status message.

Note: If the confirmation dialog is not displayed when attempting to stop the CSA service on a machine that has had users logged into it via a session of Remote Desktop Connection, the CSA service can not be stopped. The Installer hangs while displaying the "Stopping CSA" dialog. Use the Windows Task Manager to disconnect and logoff any users that are currently, or have previously been, connected to the system. Before attempting to stop CSA again, either allow the initial request to stop CSA to timeout, or reboot the system.

– If the service is running but the CSA version is not 4.5 or later, the Installer displays an error message, then exits.

– If the service is not running, and the CSA version is not 4.5 or later, the Installer displays a warning message, then provides the option to continue or not:

If you select **No**, the Installer exits.

If you select **Yes**, the installation continues.

• if features were added after the installation. If so, warnings and instructions are posted indicating the required action(s).

Figure 4: Database Schema Rollback Dialog Box
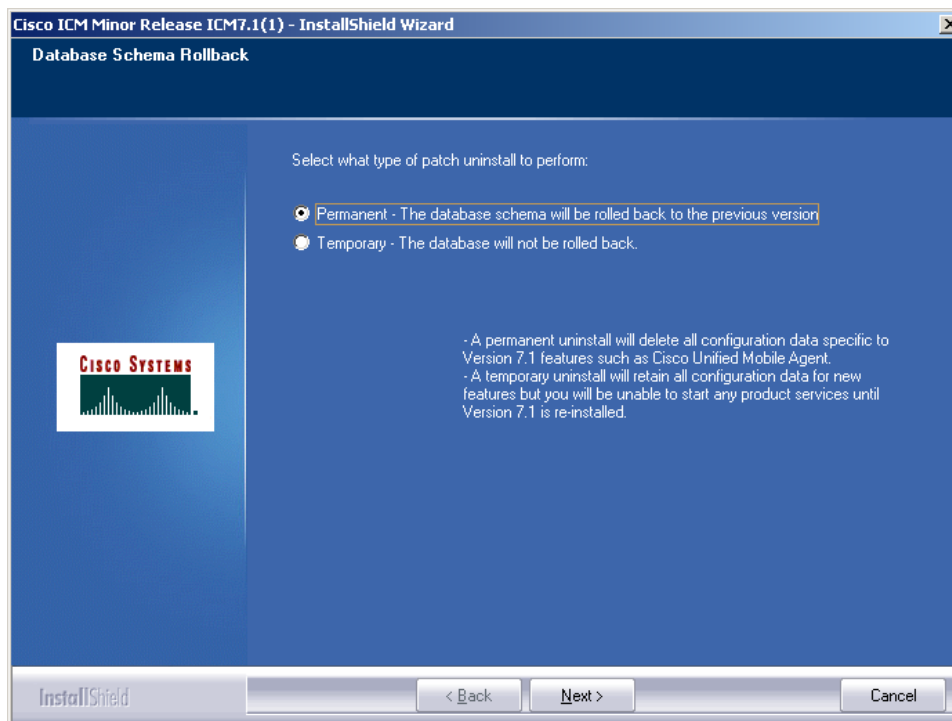
Note: Step 7 through Step 9 only appear when running an uninstallation of components with a database.

Step 7   Select **Permanent - The database schema will be rolled back to the previous version**, then click **Next**.

The Database Schema Rollback - Confirmation dialog box appears.

Step 8   Ensure you have backed up your database, then click **Yes - I have made a backup of the databases on this system.** A confirmation dialog box appears.

Step 9   Select **Yes** to continue the uninstallation.

The Setup Status dialog box appears and indicates the progress of the permanent uninstallation.

Additional messages may appear as the permanent uninstallation proceeds.

Note: If an error occurs during the permanent uninstallation process, an Uninstallation Errors dialog box appears providing error information. Once you have read the errors, click **Next** and follow the on-screen instructions.

When the permanent uninstallation is complete, the Uninstall Complete dialog box appears.

Step 10   Ensure **Yes, I want to restart my computer now** is selected (the default), then click **Finish**. After the reboot, the permanent uninstallation is complete.

After the uninstallation process has completed, and both the A and B sides of your system are operating properly, set the ICM/IPCC services that were changed from their original setting of

Automatic to **Manual** for the uninstallation back to **Automatic** to ensure that the system functions properly after a reboot.

Note: If you are not sure which services were changed from **Automatic** to **Manual** during the installation of the Release 7.1(1), examine the Messages dialog box that appears at the end of the uninstallation. You can also check the ICM Service Control.

Figure 5: Messages Dialog Box
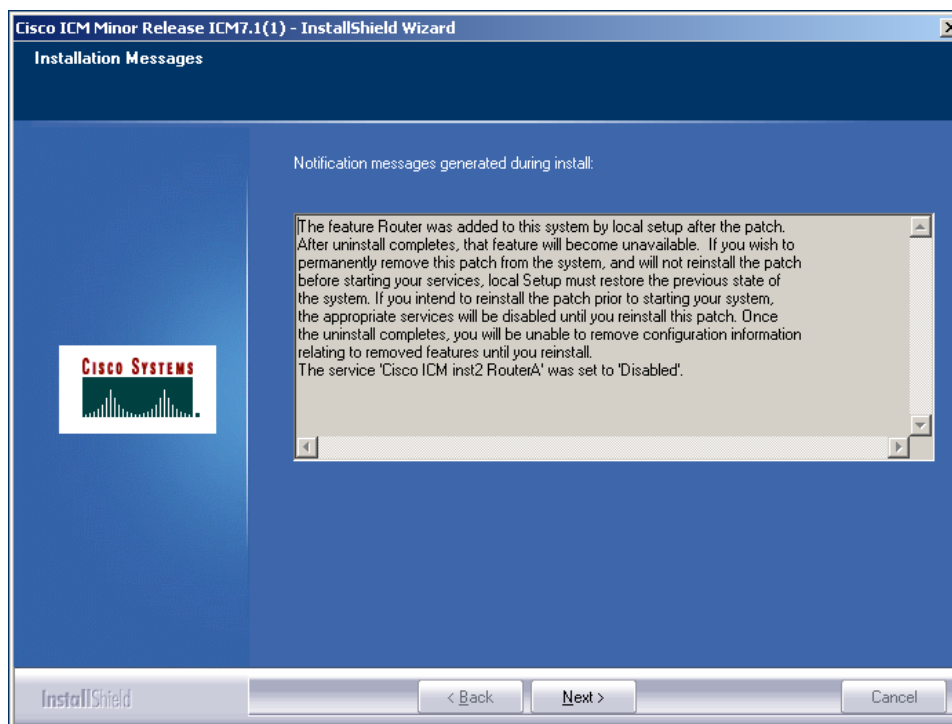
Chapter 4

Silent Installation and Manual Recovery from Installer Failures

Silent Installations

Installation programs developed with InstallShield platforms have a mechanism for running the Installer in a silent mode. In a silent installation, interactive dialogs are not displayed. Information and answers that you would normally provide are read from a response file. Response files can be identified by having the same name as the Installer executable file, but with an ".iss" extension.

Response files are created by first running the installer in "record mode". During record mode, you manually enter information the same way as if the product would be used in normal mode. To enter record mode, start the setup program from a command prompt and pass in a `/r` command line parameter. For example, if the setup program executable is setup.exe, then a response file setup.iss is created when the Installer is launched using the command `setup.exe /r`. Once the response file is created, another installation can be performed launching the Installer with the command: `setup.exe /s`.

Warning: Silent installations can be dangerous when performed with incorrect response files, and their use is discouraged. If you choose to use this method, be absolutely certain that the execution environment is configured identically to the environment where the response file was created. Slight variations in the configuration can cause unexpected errors or different installation paths that will not align with the expected response file structure. These situations could lead to a catastrophic failure of the Installer program, which, in turn, would require a manual recovery.

General Rules of Thumb for Silent Installations

- CSA must be stopped prior to creating the response file, and prior to running the installer silently.

- When running an installation silently, the system configuration must match as close as possible to the system which the response file was created on. The idea here is to minimize the potential for any unexpected dialogs during the install process. For example if the response file is created on a machine where the ICM services are set to **Manual** and then run on a machine

who's ICM services are set to **Automatic**, the installation process will display an additional dialog alerting you that the services have been set from **Automatic** to **Manual**. Since the response file was created on a machine whose services were already set to **Manual**, it will not be expecting this dialog, which will cause the installation to terminate abruptly and leave the system in an invalid state requiring a manual recovery.

- If, during the creation of the response file, you choose not to reboot the machine after the install completes, remember to manually reboot any silently installed system prior to starting the services.

- Always verify that the Installer log matches the expected results. An incomplete installation can have serious negative consequences if not properly identified.

Running a silent installation for the 7.1(1) ICM/IPCC Enterprise and Hosted Editions is a two step process:

- First, create a response file by running setup from a command prompt with two command line arguments.

  An example of the correct syntax is: `C:\>ICM7[1].1(1)_72_build_17347-Release.exe -r -f1c:\myanswerfilename.iss`

  The `-r` flag is for recording the response file.

  The `-f1` flag is the full path and filename for the resulting response file to be saved in.

  Note: There is no space between the `-f1` and the start of the file path. If no `-f1` flag is present, the response file is written to a default location.

  Once you have stepped through all of the setup process (which completes a full installation the product on the machine recording the response file) the resulting response file can be copied to any additional machine to be used during a silent installation.

- Invoke a silent installation by running setup from a command prompt with the same syntax as above, with the following exception: use `-s` instead of `-r` to indicate the installation runs silently using the response file found at `-f1filepath` (Example: `C:\>ICM7[1].1(1)_72_build_17347-Release.exe -s -f1c:\myanswerfilename.iss)`.

Verify that the silent installation completed successfully by checking the Installer log file to make sure no errors were reported, and that the Installer ran to completion.

Refer to **HOW TO: Create a Silent Installation** (http://support.installshield.com/kb/ view.asp?articleid=Q101901) (MacroVision Knowledge Base document ID: Q101901) for detailed information on how to create a silent installation.

Recovering from Unusual and Catastrophic Failures of the Installer

There are situations where the Installer may fail for reasons that cannot be anticipated or controlled.

Possible failure scenarios:

- system power loss

- system lock up due to the failure of another process

- virtual machines freezing or accidentally shut down

- silent installs using incorrect or incomplete response files

- the installer completes successfully, but you are unable to un-install using **Add/Remove Programs** in the Control Panel

Under "normal" conditions, when a failure in an InstallShield program occurs, the Installer can be aborted. An abort event is processed by InstallShield and the setup program attempts to undo the changes it has made. Changes include file deployments, registry modifications, and other modifications to Windows shell objects.

The InstallShield engine does not include native capabilities for either file backup during install or file return during uninstallation. These additional tasks are scripted enhancements made to the Windows based installer. If there is a catastrophic failure during the installation (or any other state that blocks the uninstaller program from running) the file return needs to be performed manually.

Warning: Do not attempt to repair a system by only modifying the registry and running the installation a second time. This causes you to lose the ability to return the system back to its pre-installation state. If the Installer is run a second time, it backs up the recently installed versions of files, overwriting the original files previously copied to the backup directories.

The manual recovery steps outlined below are performing a "Temporary" uninstallation. This means that files are being restored to their pre-installation (Release 7.0(0)) state, but the previous database schema is not restored. In the event of a catastrophic failure, it may not be easy to determine whether or not the proper files are in place to rollback the schema. By following the procedures listed below the system can be returned to a known state from which the Installer can be reapplied.

Backup files are stored in directories that are immediate children of the original file location. The directory name is the minor release version number with each numerical component separated by an underscore, as in ICM_7_1_1_0_0_0_44. For example, files patched in the C:\icm\bin directory are copied to a directory with a name that resembles this pattern: C:\icm\bin_ICM_7_1_1_0_0_0_44.

A list is kept in a text file for every backup directory created. This file is written to the product root directory (example: C:\icm_ICM_7_1_1_0_0_0_44\Return_ICM_7_1_1_0_0_0_44.txt).

How to Manually Return a Failed Release 7.1(1) Installation to the Pre-installation State

Perform the following steps to manually return a failed Release 7.1(1) installation:

Step 1　Locate all the backup directories using the return list file

Step 2　Copy all of the files in each backup directory to its immediate parent directory.

Step 3　Delete the backup directories and all their contents.

Note: While the deletion of the backup directories is functionally optional, it helps to keep the system clean. In the event you do delete the backup files here, it may be worthwhile to store them in a safe location elsewhere.

Step 4　Clean up the registry by removing the Installer information.

For example, the Installer information for ICM_7_1_1_0_0_0_44 is removed by deleting this key and all its contents (HKLM\SOFTWARE\Cisco Systems, Inc.\Patch\ICM\7.0\Patch\ICM_7_1_1_0_0_0_44).

Step 5　If a new language selection was made during the install, the language selection must also be reset by modifying registry named values under the key HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\SystemSettings.

a.　Copy the value of "Last Language" to "Language".

b.　Copy the value of "Last LanguageAbbrev" to "LanguageAbbrev".

While the previous instructions restores most ICM nodes, more needs to be done for a WebView deployment. WebView places many additional requirements on the Installer, such as copying files form a base repository to each WebView instance, updating templates, cleaning out caches, etc. There is no easy way to manually recover the WebView changes. However, if the manual recovery previously described is followed, the Installer may be safely applied again, and recover the WebView deployment. Once a successful installation of this minor release is deployed, the uninstallation program can be run normally to restore the WebView state to pre-installation configuration.

Chapter 5

Installing 7.1(1) Agent Desktop Software

This chapter discusses installing and uninstalling:

- Cisco Computer Telephony Integration Object Server (CTI OS), Release 7.1(1)

- Cisco Agent Desktop (CAD), Release 7.1(1)

This section contains the following topics:

Cisco Computer Telephony Integration Object Server (CTI OS), Release 7.1(1)

The installation and uninstallation of Cisco CTI OS, Release 7.1(1) is not covered in this guide. Refer to the **Cisco CTI OS System Manager's Guide for ICM/IPCC Enterprise and Hosted Edition, Release 7.1(1)** (http://www.cisco.com/en/US/products/sw/custcosw/ps14/ tsd_products_support_series_home.html) for instructions on installing and uninstalling CTI OS 7.1(1).

For additional information concerning CTI OS 7.1(1) refer to the **Release Notes** (http:// www.cisco.com/en/US/products/sw/custcosw/ps14/prod_release_notes_list.html)for this CTI OS release.

Cisco Agent Desktop (CAD), Release 7.1(1)

The installation and uninstallation of Cisco CAD, Release 7.1(1) is not covered in this guide. Refer to the **Cisco CAD Installation Guide, IP Contact Center Enterprise and Hosted Edition Release 7.1(1)** (http://www.cisco.com/en/US/products/sw/custcosw/ps427/ tsd_products_support_series_home.html) for instructions on installing and uninstalling CAD 7.1(1).

For additional information concerning CAD 7.1(1) refer to the **Release Notes** (http://www.cisco.com/en/US/products/sw/custcosw/ps427/prod_release_notes_list.html)for this CAD release.

Index