Upgrade Guide for Cisco Unified System Contact Center Enterprise
Release 7.5(1)

April 2011
Table of Contents

Preface ...........................................................................................................................................1
Purpose ..........................................................................................................................................1
Audience .........................................................................................................................................1
Organization .................................................................................................................................2
Related Documentation ..................................................................................................................4
Conventions ....................................................................................................................................4
Obtaining Documentation and Submitting a Service Request.......................................................5
Documentation Feedback .............................................................................................................5

Part 1. Unified SCCE Upgrade Preparations.....................................................................................7

1. Planning Your Unified SCCE Upgrade .......................................................................................9
   Prepare Your Upgrade Plans.........................................................................................................9
      Back Up Plans..........................................................................................................................10
      Pre- and Post-Upgrade Test Plans...........................................................................................10
   Unified SCCE Upgrade Methods ...............................................................................................11
   Network Inventory for Technology Refresh ..............................................................................12
   Schedule of Activities................................................................................................................12
   Define Upgrade Steps ..............................................................................................................13
   Default Network Route Plan .....................................................................................................13
   Plan for Hardware and Software Requirements .......................................................................14
   Compatibility Requirements ......................................................................................................14
      Component Compatibility .........................................................................................................14
   The System IPCC Enterprise Installer ....................................................................................15
      Service or Maintenance Release Requirements .....................................................................15
      Unified SCCE Enterprise Localization Support ..................................................................16
      Security Hardening ................................................................................................................16
      Registry Settings ....................................................................................................................16
      Third-Party Installers Included in the System IPCC Enterprise 7.5 Installer..........................17
   Cisco Security Agent ................................................................................................................18
   Active Directory ........................................................................................................................18
   SQL Server 2005 .........................................................................................................................18

Part 2. Unified SCCE Pre-Upgrade Tasks ......................................................................................19

2. Performing Pre-Upgrade Tasks ..................................................................................................21
   Record Current Unified SCCE Server Status ............................................................................21
      Pre-upgrade Preparation for All Unified SCCE Servers ..........................................................21
   Verify Available Disk Space ......................................................................................................22
      Calculating the amount of disk space needed for migration ..................................................22
      Configuring tempdb Log Files to Autogrow..........................................................................22
   Perform System Integrity Tests .................................................................................................24
   Perform Back Ups .......................................................................................................................24
   Perform Pre-Upgrade Tasks .......................................................................................................25
      Common Ground Pre-Upgrade Tasks ....................................................................................26
      Technology Refresh Pre-Upgrade Tasks ...............................................................................26

Part 3. Upgrading Unified SCCE .....................................................................................................29

3. Introduction to Unified SCCE Upgrade ......................................................................................31
   How Unified SCCE 7.5(1) Upgrade Works .................................................................................31
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration &amp; WebView Reporting Machines and Central Controllers</td>
<td>31</td>
</tr>
<tr>
<td>Agent/IVR Controllers</td>
<td>32</td>
</tr>
<tr>
<td>Outbound Controller</td>
<td>33</td>
</tr>
<tr>
<td>4. The Unified SCCE Upgrade Process</td>
<td>35</td>
</tr>
<tr>
<td>High Level Overview of the Upgrade Process</td>
<td>35</td>
</tr>
<tr>
<td>5. Upgrading Administration &amp; WebView Reporting Machines and Central Controllers</td>
<td>39</td>
</tr>
<tr>
<td>Common Ground Upgrade</td>
<td>39</td>
</tr>
<tr>
<td>Technology Refresh Upgrade</td>
<td>40</td>
</tr>
<tr>
<td>6. Upgrading Agent/IVR Controllers</td>
<td>43</td>
</tr>
<tr>
<td>Common Ground Upgrade</td>
<td>43</td>
</tr>
<tr>
<td>Technology Refresh Upgrade</td>
<td>44</td>
</tr>
<tr>
<td>7. Upgrading the Outbound Controller</td>
<td>45</td>
</tr>
<tr>
<td>Common Ground Upgrade</td>
<td>45</td>
</tr>
<tr>
<td>Technology Refresh Upgrade</td>
<td>45</td>
</tr>
<tr>
<td>Moving From a Standalone Outbound Controller</td>
<td>46</td>
</tr>
<tr>
<td>8. Upgrading the Multichannel Controller</td>
<td>49</td>
</tr>
<tr>
<td>Common Ground Upgrade</td>
<td>49</td>
</tr>
<tr>
<td>Technology Refresh Upgrade</td>
<td>49</td>
</tr>
<tr>
<td>9. Upgrading CTI OS Agent and Supervisor Desktop</td>
<td>51</td>
</tr>
<tr>
<td>Common Ground Upgrade</td>
<td>51</td>
</tr>
<tr>
<td>10. Upgrading Cisco Agent Desktop (CAD)</td>
<td>53</td>
</tr>
<tr>
<td>Upgrading from CAD 6.0(2) to CAD 7.5(1)</td>
<td>53</td>
</tr>
<tr>
<td>Part 4. Post-Upgrade Tasks</td>
<td>55</td>
</tr>
<tr>
<td>11. Performing Post-Upgrade Tasks</td>
<td>57</td>
</tr>
<tr>
<td>Validate the Upgrade</td>
<td>57</td>
</tr>
<tr>
<td>System Integrity Tests</td>
<td>57</td>
</tr>
<tr>
<td>Review Log Files</td>
<td>58</td>
</tr>
<tr>
<td>12. SQL Server</td>
<td>59</td>
</tr>
<tr>
<td>Upgrading from SQL Server 2000 to SQL Server 2005 - Common Ground Upgrades Only</td>
<td>59</td>
</tr>
<tr>
<td>How to Upgrade SQL Server 2000 to SQL Server 2005</td>
<td>60</td>
</tr>
<tr>
<td>Installing Microsoft SQL Server 2005</td>
<td>66</td>
</tr>
<tr>
<td>How to Install Microsoft SQL Server 2005</td>
<td>66</td>
</tr>
<tr>
<td>Appendix A. Database Tasks</td>
<td>71</td>
</tr>
<tr>
<td>Determining the Size of the ICM Database</td>
<td>71</td>
</tr>
<tr>
<td>Using ICMDBA</td>
<td>71</td>
</tr>
<tr>
<td>Using SQL Server 2000</td>
<td>71</td>
</tr>
<tr>
<td>Using SQL Server 2005</td>
<td>72</td>
</tr>
<tr>
<td>Appendix B. Exporting and Importing the Cisco Systems Inc. Registry Key</td>
<td>75</td>
</tr>
<tr>
<td>Exporting the Registry</td>
<td>75</td>
</tr>
<tr>
<td>Importing the Registry</td>
<td>76</td>
</tr>
<tr>
<td>Appendix C. Running the EDMT Wizard</td>
<td>77</td>
</tr>
<tr>
<td>Common Ground Wizard Screens</td>
<td>77</td>
</tr>
<tr>
<td>Technology Refresh Wizard Screens</td>
<td>79</td>
</tr>
<tr>
<td>Appendix D. System IPCC Enterprise Installer</td>
<td>83</td>
</tr>
<tr>
<td>Running the System IPCC Enterprise Installation Program</td>
<td>83</td>
</tr>
</tbody>
</table>
**List of Figures**

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Instance Name Dialog</td>
<td>62</td>
</tr>
<tr>
<td>2</td>
<td>Existing Components Dialog</td>
<td>63</td>
</tr>
<tr>
<td>3</td>
<td>CG Database Connection Dialog</td>
<td>78</td>
</tr>
<tr>
<td>4</td>
<td>TR Source/Destination Database Connection Dialog</td>
<td>79</td>
</tr>
<tr>
<td>5</td>
<td>TR Backup Connection/Destination Restore Location Dialog</td>
<td>80</td>
</tr>
<tr>
<td>6</td>
<td>CG Service Account Management Screen</td>
<td>84</td>
</tr>
<tr>
<td>7</td>
<td>IPCC Machine Initialization Screen</td>
<td>86</td>
</tr>
<tr>
<td>8</td>
<td>TR Service Account Management Screen</td>
<td>87</td>
</tr>
<tr>
<td>9</td>
<td>IPCC Machine Initialization Screen</td>
<td>89</td>
</tr>
</tbody>
</table>
Preface

Purpose

This guide describes the procedures for upgrading a Cisco Unified System Contact Center Enterprise (Unified SCCE) installation from Release 7.0(x), 7.1(x), and 7.2(x) to Release 7.5(1). This guide further discusses pre- and post-upgrade tasks. Because the Unified SCCE upgrade requires you to perform the upgrade procedure in an exact order, the guide also provides a high level overview of the upgrade process that outlines the acceptable step-by-step instructions. It is important that you review this procedure in advance to ensure a successful Unified SCCE upgrade.

Note: You cannot upgrade to Unified SCCE 7.5(1) from a Cisco Unified Contact Center Enterprise (Unified CCE) Release. In this case, you must perform a fresh Unified SCCE installation.

Audience

This guide is intended for the system administrators, technicians, and Cisco representatives who are responsible for the Unified SCCE upgrade.

This guide assumes that you meet the following skill set requirements:

• You have experience with the Windows Operating System
  – Active Directory
  – Security concepts
  – Network configuration and operation
• You have experience with SQL Server
– Enterprise Manager/Management Studio
– Query Analyzer
– SQL scripting

• You possess a working knowledge of Unified SCCE

– Unified SCCE machine roles (Central Controller, Agent/IVR Controller)
– Schema knowledge
– Deployment models


A Note About What's New in Unified SCCE Release 7.5(1)

In this release, Unified SCCE has been enhanced to support the following:

• Integration with Cisco Unified Customer Voice Portal (Unified CVP)

• Co-location of Outbound Controller on the Agent/IVR Controller

A Note About Product Renaming

Cisco System IPCC Enterprise Edition is being renamed Cisco Unified System Contact Center Enterprise (abbreviated as Unified SCCE).

Cisco CallManager/Cisco Unified CallManager is being renamed Cisco Unified Communications Manager (abbreviated as Unified CM).

These new names appear in this release for Agent and Supervisor product opening-screens, but they do not yet appear throughout the user interface or documentation.

Organization

The following table describes the information contained in each section of this guide:

<table>
<thead>
<tr>
<th>Part</th>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part 1. Unified SCCE Upgrade Preparations</td>
<td>Chapter 1, Planning Your Unified SCCE Upgrade (page 9)</td>
<td>Provides an overview of upgrade considerations and strategies that you can use to prepare for a Unified SCCE upgrade.</td>
</tr>
<tr>
<td>Part</td>
<td>Chapter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Part 2. Unified SCCE Pre-Upgrade Tasks</td>
<td>Chapter 2, Performing Pre-Upgrade Tasks (page 21)</td>
<td>Lists the pre-upgrade tasks that you must perform before you upgrade to Unified SCCE 7.5(1).</td>
</tr>
<tr>
<td></td>
<td>Chapter 4, The Unified SCCE Upgrade Process (page 35)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chapter 5, Upgrading the Administration &amp; WebView Reporting Machines and Central Controllers (Sides A and B) (page 39)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chapter 6, Upgrading the Agent IVR/Controller (page 43)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chapter 7, Upgrading the Outbound Controller (page 45)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chapter 8, Upgrading the Multichannel Controller (page 49)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chapter 9, Upgrading CTI OS Agent and Supervisor Desktops (page 51)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chapter 10, Upgrading Cisco Agent Desktop (page 53)</td>
<td></td>
</tr>
<tr>
<td>Part 3. Upgrading Unified SCCE</td>
<td>Chapter 11, Performing Post-Upgrade Tasks (page 57)</td>
<td>Discusses post upgrade tasks for validating the Unified SCCE upgrade.</td>
</tr>
<tr>
<td></td>
<td>Chapter 12, SQL Server (page 59)</td>
<td>Also provides procedures for installing SQL Server 2005 and upgrading SQL Server 2000 to SQL Server 2005.</td>
</tr>
<tr>
<td>Appendix A. Database Tasks</td>
<td>Appendix A. Database Tasks (page 71)</td>
<td>Provides procedures for performing database tasks.</td>
</tr>
<tr>
<td>Appendix B. Exporting and Importing the Cisco Systems, Inc Registry Key</td>
<td>Appendix B. Exporting and Importing the Cisco Systems, Inc Registry Key (page 75)</td>
<td>Provides procedures for exporting and importing the Cisco Systems, Inc registry.</td>
</tr>
<tr>
<td>Appendix C. Running the EDMT Wizard</td>
<td>Appendix C. Running the EDMT Wizard (page 77)</td>
<td>Provides procedures for running the EDMT wizard.</td>
</tr>
<tr>
<td>Appendix D. Cisco IPCC Enterprise Installer</td>
<td>Appendix D. Cisco IPCC Enterprise Installer (page 83)</td>
<td>Provides procedures for using the Installer.</td>
</tr>
<tr>
<td>Appendix E. Uninstalling Unified SCCE</td>
<td>Appendix E. Uninstalling Unified SCCE (page 93)</td>
<td>Provides procedures for uninstalling Unified SCCE.</td>
</tr>
</tbody>
</table>
Related Documentation

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

- The Installation and Configuration Guide for Cisco Unified System Contact Center Enterprise (Unified SCCE) provides information to help you understand, install, and configure the System deployment of Cisco Unified Contact Center Enterprise. You can access this guide from http://www.cisco.com/en/US/products/sw/custcs/wps1844/prod_installation_guides_list.html


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/web/psa/products/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:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example:</td>
</tr>
<tr>
<td></td>
<td>• Choose Edit &gt; Find.</td>
</tr>
<tr>
<td></td>
<td>• Click Finish.</td>
</tr>
<tr>
<td><strong>italic</strong> font</td>
<td>Italic font is used to indicate the following:</td>
</tr>
</tbody>
</table>
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:


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.
Part 1: Unified SCCE Upgrade Preparations

This section provides an overview of upgrade strategies and considerations that you can use to prepare for a Unified SCCE upgrade.
Planning Your Unified SCCE Upgrade

There are several areas of concern to consider when you plan a Unified SCCE upgrade. This document provides detailed information and references to help you plan properly for a successful upgrade.

This chapter contains the following topics:

- Prepare Your Upgrade Plans, page 9
- Plan for Hardware and Software Requirements, page 14
- Compatibility Requirements, page 14
- The System IPCC Enterprise Installer, page 15
- Cisco Security Agent, page 18
- Active Directory, page 18
- SQL Server 2005, page 18

Prepare Your Upgrade Plans

Typically, there is a limited maintenance window in which to perform an upgrade. When there are a large number of servers in your deployment, it may not be possible for you to upgrade all of the servers in one maintenance window.

Before starting an upgrade of your Unified SCCE system, it is strongly recommended that you first prepare and access your upgrade plans.

Your upgrade plan considerations should include:

- Back up plans
- Pre- and post-upgrade test plans
- Unified SCCE upgrade methods
- Network inventory for technology refresh
When planning your Unified SCCE upgrade, it is necessary for you to also consider the additional software that interfaces with the Unified SCCE software.

Examples of the additional software include, but are not limited to:

- Cisco Unified Communications Manager (Cisco Unified CM) and Cisco Unified IP IVR (Unified IP IVR) or Cisco Unified Customer Voice Portal (Unified CVP)

  **Note:** If you have upgraded to Cisco Unified Communications Manager 5.0, you must upgrade the JTAPI client software on any application server (such as, Agent/IVR Controller) or client workstation on which JTAPI applications are installed. If you do not upgrade the JTAPI client, your application will fail to initialize.

- Cisco CTI desktop/client
- Cisco Unity
- Cisco Personal Assistant
- Cisco Unified CM Auto-Attendant
- Recording solutions
- Cisco Agent Desktop

**Back Up Plans**

Release 7.5 upgrade does not have roll back functionality. While not required, it is a best practice to perform full system backups prior to this upgrade. The backup will be useful if, at any point, a downgrade is necessary.

While you might normally perform regularly 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.

See **Perform Back Ups (page 24)** for a more detailed explanation about backups.

**Pre- and Post-Upgrade Test Plans**

At the beginning of the maintenance window, consider creating a pre-upgrade test plan to establish the benchmark. The benchmark is used when you run the post upgrade tests that you develop to test your Unified SCCE system during various stages of the upgrade process. It is your responsibility to develop actual test cases and outline the expected results.
In addition, be sure to schedule appropriate resources to ensure any custom CTI functionality is operational after an upgrade.

See Perform System Integrity Tests (page 24) for a more detailed explanation about testing during the upgrade process.

See Post Upgrade Tasks (page 57) for additional information.

Unified SCCE Upgrade Methods

Unified SCCE 7.5 supports two upgrade methods:

- **Common Ground (CG)**

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

  The Common Ground upgrade procedure migrates the Logger (ipcc_side<A/B>) and HDS database (ippc_hds) in-place and updates the existing database schema modified from System IPCC 7.(x) to Unified SCCE 7.5.

- **Technology Refresh (TR)**

  A Technology Refresh upgrade is performed when you decide to (or it is required that you) upgrade your hardware as well as your Cisco Unified ICM/Contact Center Enterprise software and supporting third party software.

  A Technology Refresh transports all data, customized files, and related registry keys to the new hardware previously configured with a compatible operating system and database server (where required).

  It is not necessary to perform manual system backups during the Technology Refresh as the source machines remain unchanged.

Regardless of the upgrade method you choose, there are pre-upgrade tasks that you must perform to ensure a successful upgrade. You must also run the Enhanced Data Migration Tool (EDMT) to upgrade a System IPCC 7.x, Logger and HDS database to the ICM/Unified SCCE 7.5(1) database schema package.

This release supports a combination of Common Ground migration on some Unified SCCE nodes and Technology Refresh on others. However, upon completion of upgrade, it is important that side A and side B of any given component are running on identical hardware.

**See Also**

Perform Pre-Upgrade Tasks (page 21)

High Level Overview of the Upgrade Process (page 35)
Network Inventory for Technology Refresh

Technology Refresh upgrade planning and execution requires that you draw a comprehensive and accurate system diagram detailing the Unified SCCE production system’s private and visible networks.

The private network is dedicated for Central Controller node communication and is 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 Central Controller to the recovering side Central Controller

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 requests
- Central Controller database recovery
- Heartbeats – messages sent every 100 milliseconds to the Router and the Peripheral Gateway (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.

Schedule of Activities

Due to the complexity of upgrading a Unified SCCE production system, consider creating a detailed schedule of upgrade activities. This allows your project manager to maintain the status of each machine upgrade. It might also help to use a chart indicating all of the Unified SCCE 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 Central Controllers and Administration & WebView Reporting machines upgraded first. After upgrading your Central Controllers and Administration & WebView Reporting machines, you must upgrade your Agent/IVR Controller(s), and Outbound Controller and Multichannel Controller (if deployed) at your earliest convenience. Until that time, they will continue to
function properly, but they may not be reconfigurable from the Web Administration Tool until the entire Unified SCCE upgrade is complete.

It is important to notify the following Unified SCCE associated personnel of all upgrade activities and schedules.

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

Define Upgrade Steps

The upgrade migration of a Unified SCCE system involves numerous steps. From your initial software load, you may perform operating system maintenance, the Unified SCCE software upgrade (and options), the recommended database software upgrades, and additional required third-party software.

Be aware that, for a period of time during the upgrade migration, Unified SCCE 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.

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 decide whether to proceed with the upgrade of 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 while side B remains in service.

Default Network Route Plan

It is recommended that you have a default routing plan in place prior to the upgrade date and start time.

When you cross over from your old System IPCC production system to your new Unified SCCE system, the production system is shut down for a short period of time until the cross over is complete. It takes just a few minutes to do the cross over. This cross over is the only point in the upgrade process where the system does not route calls. The default network route plan is the method used to route calls during this period of time. Improper planning for cross over has definite negative consequences. Both sides of a duplexed pair cannot run at the same time with different versions of ICM software, so be sure that the first side is completely stopped before you start the upgraded side.
Plan for Hardware and Software Requirements

Hardware specifications play a critical part in the successful operation of a Unified SCCE system. Consider auditing all servers prior to the upgrade to determine whether a hardware upgrade is required.


Before you upgrade, you should make note of all hardware and related software requirements.

Other upgrade planning considerations

- The Windows Firewall configuration scripts must be deployed before Unified SCCE servers can accept network connections.

- **Note:** The 7.x system components must be functional prior to upgrade.

- **Note:** If you intend to reuse existing hardware, 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.

**Note:** Refer to the [Cisco IP Contact Center Enterprise Edition Software Compatibility Guide](http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_device_support_tables_list.html) for the compatibility between the Cisco Unified CM version and the Unified IP IVR or Unified CVP version.

Compatibility Requirements

Component Compatibility

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 Central Controllers and Administration & WebView Reporting machines upgraded first. After upgrading your Central Controllers and Administration & WebView Reporting machines, you need to upgrade your Agent/IVR Controller(s), and Outbound Controller and Multichannel Controller (if deployed) at your earliest convenience. Until that time, they will continue to function properly, but they may not be reconfigurable from the Web Administration Tool until upgrade is complete.

To minimize upgrade complications and keep components synchronized, you need to upgrade your components to the same release of software as the Central Controller.
For example, if you upgrade your Central Controller servers to Release 7.5(1), you must upgrade your Administration & WebView Reporting machines, Outbound Controller servers, and Multichannel Controller servers to Release 7.5(1) as well. Note that enabling the Outbound Controller on the Agent/IVR Controller requires that you first complete the Agent/IVR Controller upgrade.

The following are the machine roles with their ICM equivalents:

- Central Controller = Router + Logger
- Administration & WebView Reporting = Configuration Tools + Distributor AW + WebView + HDS + Internet Script Editor server
- Agent/IVR Controller = IPCC System Peripheral Gateway (PG) + CTI Server + CTI OS Server. VRU PG is optional and used when CVP is deployed.
- Outbound Controller = Media Routing PG for Outbound + Dialer
- Multichannel Controller = Media Routing PG for Cisco Interaction Manager (CIM)

Refer to the Hardware and System Software Specification (Bill of Materials) for Cisco Unified ICM/Unified Contact Center Enterprise & Hosted, Release 7.5(1) for detailed information about hardware and system software compatibility.

The System IPCC Enterprise Installer

Upgrade functionality is built into the Unified SCCE 7.5(1) installation software so that you only need to run a single installer to perform either a fresh installation or an upgrade of an existing 7.x system.

The System IPCC Enterprise Installer upgrades all of the applicable files for each machine's intended role in the deployment. The upgrade also retains user-configured settings (such as registry entries and configuration files), as applicable.

Note: Unified SCCE can NOT exist on the same machine on which Unified ICME or Unified CCE is installed. If the installer detects that the system currently has a deployment of Unified ICME or Unified CCE installed on it, an error displays and the installer aborts. You must run ICM Setup to upgrade that machine. If you want to retask the machine for a System deployment of Unified CCE, you must start with a fresh Operating System installation.

Service or Maintenance Release Requirements

You do not need to manually remove service or maintenance release software before upgrading.

At the time of this publication, the System IPCC Enterprise installer supports upgrade when the following patches are installed. Each is a cumulative patch that includes the functionality of all previously released patches.

- 7.0 SR4 Service Release
• 7.1(5) Maintenance Release

• 7.2(5) Maintenance Release

When the System IPCC Enterprise installer detects a valid set of patches on your system, it removes any trace of the patch from the registry and from the Add/Remove Programs list. The old code is replaced with the new, updated code. There is no further action required on your part.

Unified SCCE Enterprise Localization Support

If you are upgrading a System IPCC system that has applied localized components from the 7.x Patch Installer, Unified SCCE 7.5 will upgrade the localized files automatically during the upgrade process.

Unified SCCE 7.5(1) introduces the addition of the Language Pack, which contains all of the localized files supported in this release. The Language Pack Installer for Unified Contact Center Enterprise (CCE) 7.5(1) is a separate program from Unified CCE Setup. International customers performing a new installation of Unified SCCE need to run Language Pack to install the localized components.

Refer to the Hardware and System Software Specification (Bill of Materials) for Cisco Unified ICM/Unified Contact Center Enterprise & Hosted, Release 7.5(1) for a list of supported localized versions of Microsoft Windows and SQL Server that may be used with System IPCC.

Refer to the Installation and Configuration Guide for Cisco Unified System Contact Center Enterprise 7.5(1) for detailed language pack installation instructions.

Security Hardening

During an upgrade, the System IPCC Enterprise installer determines whether Cisco ICM Operating System Security Hardening was previously applied.

If the Cisco ICM security template exists on the system, the installer automatically upgrades the template and prompts you to apply new security settings during the upgrade. You can choose to apply Security hardening changes during the upgrade or any time thereafter.

Use the Security Wizard to manually install the latest Cisco ICM security settings template at your discretion. Refer to the Security Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 7.5(1) for more information about security hardening.

Registry Settings

Prior to upgrading the registry, the System IPCC Enterprise installer makes a copy of the ICM registry and saves it on the local machine at <target disk>:\ICM\backup\<Date and Time string>.
The backup snapshot of the registry is named \texttt{SIPCCRegistry.reg.txt}. It has an extension of \texttt{.reg.txt} so that if you open it, it does not overwrite the new registry with old values. In addition, if you run the upgrade multiple times, the registry is saved for each snapshot in time.

\textbf{Note:} It is the responsibility of the customer, partner, TAC engineer, and/or software engineer to manually remove any unnecessary registry settings that may have been added temporarily. Additionally, if trace settings have been altered, when the debug session is complete the person responsible for the changes needs to reset trace settings to ensure the performance of the system is not impaired.

See \textit{Perform Back Ups (page 24)} for a more detailed explanation about backups.

Third-Party Installers Included in the System IPCC Enterprise 7.5 Installer

The installation/upgrade software bundles and silently calls the installers of the following third party software:

\begin{itemize}
  \item CTI OS Server 7.5(1)
  
  The System IPCC Enterprise installer upgrades CTI OS Server 7.x(y) to CTI OS Server 7.5(1). The CTI OS Server resides on your Agent/IVR Controller. No manual configuration of this component is necessary for upgrade.
  
  \item Support Tools 2.3(1)
  
  The System IPCC Enterprise installer automatically upgrades the Support Tools Node Agent to version 2.3(1).
  
  \textbf{Note:} Before upgrading any of the System IPCC Core components (using either the Technology Refresh or the Common Ground method), upgrade the existing ICM Support Tools server to version 2.3. This is required for compatibility with the Version 2.3 Support Tools agents that are installed on the Unified SCCE nodes during the upgrade process. The Version 2.3 Support Tools server is compatible with older Support Tools agents.
  
  When an IPSEC key is present, Support tools upgrades silently and is enabled by default. If the IPSEC key is not present, the System IPCC Enterprise installer prompts you for the key. Keys are case-sensitive and limited to 256 characters. You can use any character except single and double quotation marks ("), back slash(\), and pipe(|). There is no default value for the IPSEC key.
  
  \item JDK/SDK 1.5.0_14
  
  \item Apache Tomcat is upgraded to version 5.5.25.
  
  \item Microsoft .NET framework version 3.5
  
  \item WebView third-party tools
  
  Sybase EAServer and New Atlanta Servlet Exec have not changed since Release 7.0; they are not upgraded.
\end{itemize}
Cisco Security Agent

The Cisco IPCC Enterprise 7.5(1) Installer requires that, if installed, the Cisco Security Agent (CSA) software be version 5.2. The CSA policy used for Unified SCCE is the same as that used for ICM and CTI OS Server.

In this release, the Cisco IPCC Enterprise Installer automates the stopping and starting of the CSA service. If the installer detects a running instance of CSA, it automatically stops the service. CSA is automatically restarted and enabled when the upgrade completes.


Refer to the Hardware and System Software Specification (Bill of Materials) for Cisco Unified ICM/Unified Contact Center Enterprise & Hosted, Release 7.5(1) for detailed information about third party software version requirements.

Refer to the Cisco Security Agent Installation/Deployment Guide for Cisco Unified Customer Voice Portal, Release 7.5(1) for more information about how to upgrade, disable, or reenable the CSA service.

Active Directory

Unified SCCE 7.5(1) components require that a Windows Active Directory environment (whether corporate or dedicated to the Unified SCCE applications) be configured and staged prior to upgrade. See the Staging Guide for Cisco ICM/Unified Contact Center Enterprise & Hosted for further specifics on Active Directory configuration and other network configuration requirements. Additional network consideration and planning guidelines can be found in the Cisco Unified Contact Center Enterprise 7.5 Solution Reference Network Design Guide.

SQL Server 2005

SQL Server 2005 is supported with this release. SQL Server 2000 will be supported, but only for a 90-day transition period. Specific requirements and recommendations, for new installations, technology refresh upgrades, and common ground upgrades, are found in the Hardware and System Software Specification (Bill of Materials) for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 7.5(1). The 'Dynamic' memory setting is recommended for Logger and HDS.

Refer to the SQL Server (page 59) for instructions on upgrading from SQL Server 2000 to SQL Server 2005.
Part 2: Unified SCCE Pre-Upgrade Tasks

This section lists the pre-upgrade tasks that you need to perform before you upgrade Unified SCCE.
Performing Pre-Upgrade Tasks

This section discusses the pre-upgrade tasks that are recommended to ensure a successful Unified SCCE upgrade.

This chapter contains the following topics:

- Record Current Unified SCCE Server Status, page 21
- Verify Available Disk Space, page 22
- Perform System Integrity Tests, page 24
- Perform Back Ups, page 24
- Perform Pre-Upgrade Tasks, page 25

Record Current Unified SCCE Server Status

Pre-upgrade Preparation for All Unified SCCE Servers

Pre-upgrade preparation is an integral part of the upgrade process. Consider performing the following on all Unified SCCE 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.
Verify Available Disk Space

The Enhanced Data Migration Tool (EDMT) is standalone software used to upgrade a System IPCC 7.x Logger and HDS database to the Unified SCCE 7.5(1) database schema package.

EDMT requires additional disk space in which to copy and modify data and data structures during the migration process. Additional disk space must be available to the database to allow the database, database log file, tempdb, and tempdb log file to grow.

Calculating the amount of disk space needed for migration

To calculate the amount of disk space needed, perform the following steps.

**Step 1** Use the ICMDBA tool (page 71) to gather database information.

**Step 2** Open the database and select Properties.

*Note:* The Database Used Size (DUS) = Percent Used of the Data Size Value.

**Step 3** Calculate the required disk space for the migration.

- Determine the DUS
- Determine the required disk space for the database migration where:

  \[
  \text{Required Disk Space} = 120\% \times \text{DUS}
  \]

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

- **Database Used Space (DUS) = 71,680 MB**
- **Required Database Size = (1.2\times 71,680) = 86,016 MB**

Configuring tempdb Log Files to Autogrow

The Temp DB Log must be able to expand to 3 GB.

To ensure the TempDB data size is able to expand to 3 GB of the DUS calculated previously, perform the following steps as appropriate for your version of SQL Server.

*Note:* SQL Server 2005 is supported with this release. SQL Server 2000 is also supported, but only for a 90-day transition period.

If using SQL Server 2000, perform the following steps:
1. Run SQL Server Enterprise Manager and from the list of databases on the destination system, right-click tempdb and select Properties.

2. Select the Transaction Log tab.

3. Ensure the Automatically grow file check box is selected.

4. In the File Growth box, select In megabytes and set a value of 500.

5. In the Maximum File Size box, select Restrict file growth (MB) and set a value of 3072.

6. Click OK.

If using SQL Server 2005, perform the following steps:

1. Run SQL Server Management Studio.

2. From the System Databases on the destination system, right-click tempdb and select Properties.

3. From the side panel, select Files.

4. If the templog database file size is less than 500 MB, click Add.

5. Create a new unique Logical Name, such as templog1.

6. Select File Type of Log.

7. Click ... button to display the Change Autogrowth dialog box.

8. Ensure the Enable Autogrowth check box is selected.

9. In the File Growth, select In Megabytes and enter a value of 500.

10. In the Maximum File Size box, select Restricted File Growth (MB) and enter a value of 3072.

11. Click OK to confirm the Autogrowth value modifications and dismiss the autogrowth dialog box.

12. On the Database Properties dialog box, click OK to modify the tempdb log sizes.

See Also

Database Tasks (page 71)
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

Perform Back Ups

Back up is an integral part of the pre-upgrade preparation. The System IPCC Enterprise installer offers to back up the database if it is larger than 5GB. Otherwise, the database is automatically backed up; user-configurable files and registry settings are also backed up and saved on the local machine at <target disk>:\ICM\backup\<Date and Time string>. It is, however, always a good idea to manually back up your data. You might also consider copying the backup files to a different machine, preferably at a different location. The customer always assumes all security and backup management responsibilities.

**Note:** If, for some reason, you need to revert to an earlier release, it is important that you restore the database from the backup you performed prior to running EDMT. Do not use the database backups that the System IPCC Enterprise installer creates as these backups have already been upgraded to the new release version.

The following table lists the system critical data that you must back up and restore, copy and paste, or export and import (based upon the upgrade migration method you select).

**Note:** Cisco strongly recommends that you consider creating bootable images of the system that include the operating system and the network configuration. Performing this type of backup is a good business practice and helps to ensure system recovery in case catastrophic conditions occur during the upgrade process.

<table>
<thead>
<tr>
<th>System Critical Data</th>
<th>Common Ground Upgrade</th>
<th>Technology Refresh Upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup the Logger SQL Server database(s).</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Backup the Historical Data Server (HDS) SQL Server database(s).</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
## Perform Pre-Upgrade Tasks

Unified SCCE 7.5 supports two distinct approaches for upgrading an existing System IPCC installation to the 7.5 release of the software; Common Ground and Technology Refresh. Regardless of the approach you choose, you *must* perform the pre-upgrade tasks to ensure a successful upgrade.

This guide refers to the current 7.x machines as the *source* machines. New Unified SCCE 7.5 machines are referred to as the *destination* machines.

- **Common Ground (CG) Upgrade**

  The Common Ground upgrade is performed in-place on existing hardware that meets the minimum requirements for Release 7.5(1).

  A Common Ground upgrade uses EDMT to migrate the Logger (ipcc_side<A/B>) and HDS database (ippc_hds) in-place and updates the existing database schema modified from System IPCC 7.(x) to Unified SCCE 7.5.

- **Technology Refresh (TR) Upgrade**

  The Technology Refresh upgrade is performed on newly acquired hardware. This upgrade approach migrates historical and configuration data from the prior hardware deployment.

  It is not necessary to perform manual backups during the Technology Refresh as the source machines will remain unchanged.

  A Technology Refresh upgrade uses EDMT to back up the database on the source system to a network share. The database is restored on the destination system; it is then upgraded as though it were a Common Ground upgrade. Technology Refresh also uses the Service Account Management to configure Active Directory service accounts.

### System Critical Data

<table>
<thead>
<tr>
<th>System Critical Data</th>
<th>Common Ground Upgrade</th>
<th>Technology Refresh Upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup any custom databases.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Backup WebView database on the Administration &amp; WebView Reporting machine(s).</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Export the Cisco Systems, Inc. registry key on all production system nodes.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>WebView users must backup custom templates. The custom templates are in the \ICM&lt;instance&gt;\AW\custom directory on the Administration &amp; WebView Reporting machine(s).</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Back up the Outbound database on the Side A Central Controller if the Outbound option is deployed.</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
**Note:** Cisco recommends that you retain the IP addresses and machine names of your source machines and reuse the names on your new destination machines. This practice helps to maximize system uptime and reduce system reconfiguration.

## Common Ground Pre-Upgrade Tasks

Perform the following steps for a Common Ground upgrade.

### Step 1
Perform a full SQL Server backup of the following databases.

<table>
<thead>
<tr>
<th>Server</th>
<th>Database</th>
<th>Database name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Controller sides A &amp; B</td>
<td>Logger</td>
<td>ipcc_side\A/B &gt;</td>
</tr>
<tr>
<td>Administration &amp; WebView Reporting machine</td>
<td>Historical Data Server</td>
<td>ipcc_hds</td>
</tr>
</tbody>
</table>

### Step 2
Use the Registry Editor to export the Cisco Systems, Inc registry on each machine.

### Step 3
Disable configuration changes.

a. Set the HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc\ICM\IPCC\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance key to 1 on both sides of the Central Controller.

**Note:** RouterA in the registry key above is RouterB on the Side B Central Controller.

b. Verify that configuration changes are disabled by attempting to save a configuration change.

The following message displays to assure you that configuration changes are disabled: *Unable to establish a database connection for update operations*.

### Step 4
On machines that have an Administration & WebView Reporting machine or Central Controller, use SQL Server management tools to locate the tempdb database and perform the following steps:

a. click the DataFiles tab.

b. under File Properties, select Automatically Grow File.

c. under Maximum File Size, ensure that the Unrestricted file growth check box is selected.

d. click OK.

## Technology Refresh Pre-Upgrade Tasks

In the following procedure, we refer to the current 7.x machines as the *source* machines. New Unified SCCE 7.5 machines are referred to as the *destination* machines.
Perform the following steps for a Technology Refresh upgrade:

---

**Step 1** Disable configuration changes on the source Central Controllers.

a. Set the `HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc\ICM\IPCC\RouterA\Router\Current\Version\Configuration\Global\DBMaintenance` key to 1 on both sides of the Central Controller.

b. Verify that configuration changes are disabled by attempting to save a configuration change.

The following message displays to assure you that configuration changes are disabled: *Unable to establish a database connection for update operations.*

**Step 2** Use the **Registry Editor** to export the **Cisco Systems, Inc** registry on each source machine.

**Step 3** Import the registry file on each corresponding destination machine.

**Step 4** On destination Administration & WebView Reporting machines or Central Controllers, use **SQL Server management tools** to locate the **tempdb** database and perform the following steps:

a. click the **DataFiles** tab.

b. under **File Properties**, select **Automatically Grow File**.

c. under **Maximum File Size**, ensure that the **Unrestricted file growth** check box is selected.

d. click **OK**.
Part 3: Upgrading Unified SCCE

This section contains the procedures for performing Common Ground and Technology Refresh upgrades.
Introduction to Unified SCCE Upgrade

Unified SCCE deployment is comprised of several individual components or nodes that can be geographically dispersed. The Unified SCCE upgrade allows the full system to be upgraded over multiple maintenance windows.

Upgrading to Unified SCCE 7.5 involves numerous steps, more importantly, the order in which you perform the upgrade steps must be exact. From your initial software load, you may need to upgrade the operating system, the Unified SCCE software (and options), the database software, and any required third-party software.

After you upgrade your Administration & WebView Reporting machines and Central Controllers Cisco recommends that you upgrade your Agent/IVR Controllers, and Outbound Controller and Multichannel Controller (if deployed) at your earliest convenience. Until that time, these components will continue to function properly, but may not be reconfigurable from the Web Administration tool until upgrade is complete.

Caution: Running the System IPCC Enterprise Installer over the network is unsupported. You must either run the Installer from the installation media (DVD) or copy the Installer directory to the target machine and then run from the local machine. Various and miscellaneous errors can occur during installation over the network. It is also important to remember that Release 7.5(1) is a full installation and that there is no automated rollback.

How Unified SCCE 7.5(1) Upgrade Works

Administration & WebView Reporting Machines and Central Controllers

An upgrade begins with the Administration & WebView Reporting machines and Central Controllers. To ensure that your production machines continue to run without interruption, Cisco recommends that you upgrade the A side of each component first and then each component’s B side.
Performing an upgrade of the Administration & WebView Reporting machines and Central Controllers—sides A and B—is a four-part process. In other words, you will repeat the steps for performing an upgrade a total of four times beginning with the Administration & WebView Reporting server whose preferred side is the side A Central Controller.

To minimize downtime and ensure server availability, an upgrade must progress in the following order.

1. Administration & WebView Reporting machine (that will connect to the A side Central Controller)
2. A side Central Controller
3. Administration & WebView Reporting machine (that will connect to the B side Central Controller)
4. B side Central Controller

Agent/IVR Controllers

An Agent/IVR Controller consists of the IPCC System PG, CTI OS Server and CTI Server.

Upgrading Agent/IVR Controllers is done in much the same manner as the Administration & WebView Reporting machines and Central Controllers. Upgrading the Agent/IVR Controllers (sides A and B) is a two-part process. You will upgrade the A side Agent/IVR Controller first and then the B side Agent/IVR Controller. Here again, it is important that you follow the upgrade process exactly to minimize downtime and ensure server availability.

The A and B side Agent/IVR Controllers must be upgraded within the same maintenance window, along with the standalone Outbound Controller if Outbound is deployed and you are choosing to keep the Outbound Controller on its own machine.

New IVR Functionality in Release 7.5(1)

In Unified SCCE Release 7.5(1), IVR functionality is provided by either Cisco Unified IP IVR (Unified IP IVR) or Cisco Unified Customer Voice Portal (Unified CVP). Both Unified IP IVR and Unified CVP are multichannel (voice, data, and Web) IP-enabled IVR applications. Unified CVP is a VoiceXML-based solution that provides carrier-class IVR and IP switching services on Voice over IP (VoIP) networks.

Unified SCCE 7.5(1) supports Unified CVP versions 4.0(2), 4.1, and 7.0(1). Note that the System IPCC Enterprise Installer does not install or upgrade any CVP components because CVP is packaged separately.

After upgrading Unified SCCE, you can opt to change the deployed IVR from IP IVR to CVP. Installing and configuring CVP is a large undertaking and requires detailed pre-planning. When you are ready to make the switch from IP IVR to CVP in Unified SCCE, launch the IPCC Enterprise Web Administration tool and navigate to the System Management > Machine...
Management > Machines page. Run the machine wizard for BOTH Agent/IVR Controllers, changing the deployed IVR to CVP on the IVR Connectivity page, and finish the wizard.

Refer to the following documentation for instructions on installing and configuring Unified Customer Voice Portal (Unified CVP).

- Configuration and Administration Guide for Cisco Unified Customer Voice Portal


Note: Switching to Unified CVP requires that you first complete the Agent/IVR Controller upgrade.

Outbound Controller

The Outbound Controller consists of the Outbound Dialer, and the Media Routing (MR) PG used by Outbound.

New in the Unified SCCE Release 7.5(1), you can choose to co-locate the Outbound Controller on the Agent/IVR Controller in your deployment. Co-location reduces box count and simplifies the overall deployment without affecting performance. Another benefit of co-locating is that the MR PG is duplexed and you get more Dialer ports by adding an additional Dialer on the B side Agent/IVR Controller.
How Unified SCCE 7.5(1) Upgrade Works
Chapter 4

The Unified SCCE Upgrade Process

As a precaution, it is always recommended that a recovery plan be mapped out prior to the start of the Unified SCCE upgrade. If a failure occurs (for example, software, hardware), back out and recovery time must be considered. If a failure does occur, it is likely to happen during the upgrade of the first Administration & WebView Reporting machine and A side Central Controller. These are steps one through seven within the upgrade sequence.

The upgrade process is summarized in the following step procedures. These steps are intended as a high level overview of the upgrade process. You will need to follow the corresponding links to locate component specific upgrade instructions.

**Caution:** To ensure a successful upgrade and minimize downtime, you MUST perform the upgrade procedures in the exact order documented in this guide.

High Level Overview of the Upgrade Process

**Note:** With exception of step 7 only, you will use the Web Administration Tool to start and stop services when instructed. Only step 7 requires you to use Windows Services to start services on the Administration & WebView Reporting machine (whose preferred Central Controller is the A side) and the A side Central Controller.

**Step 1**
Be sure you have performed the pre-upgrade tasks (page 26).

- For a *Common Ground* upgrade, see Pre-upgrade Tasks for Common Ground Upgrade (page 26)
- For a *Technology Refresh* upgrade, see Pre-upgrade Tasks for Technology Refresh Upgrade (page 26)

**Step 2**
Stop services on the **Administration & WebView Reporting machine** (Distributor) whose preferred Central Controller is the *A side Central Controller*.

**Step 3**
Upgrade the **Administration & WebView Reporting machine** on which services are stopped.
• To perform a *Common Ground* upgrade, see [Common Ground Upgrade](page 39)

• To perform a *Technology Refresh* upgrade, see [Technology Refresh Upgrade](page 40)

**Step 4**
On the running Administration & WebView Reporting machine, launch the Web Administration tool and navigate to *Service Management*, then stop services on the **A side Central Controller**.

**Step 5**
Upgrade the **A side Central Controller**.

• To perform a *Common Ground* upgrade, see [Common Ground Upgrade](page 39)

• To perform a *Technology Refresh* upgrade, see [Technology Refresh Upgrade](page 40)

**Step 6**
Stop services on both the **Administration & WebView Reporting machine** whose preferred Central Controller is the **B side Central Controller** and the **B side Central Controller**.

**Step 7**
Bring up services on both the **Administration & WebView Reporting machine** whose preferred Central Controller is the **A side Central Controller** and the **A side Central Controller**.

**Note:** For this step only, use Windows Services to start services on the Administration & WebView Reporting machine (whose preferred Central Controller is the A side) and the A side Central Controller.

**Caution:** If a failure does occur, it is likely to be apparent at this point. Cisco recommends that you perform a preliminary verification of the upgrade to verify the upgraded machines are functioning properly.

**Step 8**
Launch the ICM/IPCC Enterprise Web Administration tool (on the upgraded Administration & WebView Reporting server) and choose *System Management > Machine Management > Machines*. Verify that all of the machines in your deployment are listed.

If A side operations fail, *do not* proceed further. Revert to the B side machines and troubleshoot A side operations before continuing with upgrade procedures.

**Step 9**
Upgrade the **Administration & WebView Reporting machine** whose preferred Central Controller is the **B side Central Controller**.

• To perform a *Common Ground* upgrade, see [Common Ground Upgrade](page 39)

• To perform a *Technology Refresh* upgrade, see [Technology Refresh Upgrade](page 40)

**Step 10**
Upgrade the **B side Central Controller**.

• To perform a *Common Ground* upgrade, see [Common Ground Upgrade](page 39)

• To perform a *Technology Refresh* upgrade, see [Technology Refresh Upgrade](page 40)

**Step 11**
Start services on the **B side Central Controller**.

**Step 12**
Start services on the **Administration & WebView Reporting machine** whose preferred Central Controller is the **B side Central Controller**.
Step 13  Enable configuration changes.

   a. Set the \HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc\ICM\PCC\Router\A/B\Router\CurrentVersion\Configuration\Global\DBMaintenance key to 0 on both sides of the Central Controller.

   b. Verify that configuration changes are enabled.

   Note: This is an acceptable place to stop an initial maintenance window. After upgrading your Administration & WebView Reporting machines and Central Controllers, you must upgrade your Agent/IVR Controller(s), Outbound Controller, and Multichannel Controller (if deployed) at your earliest convenience. Until that time, they will continue to function properly, but may not be reconfigurable from the Web Administration Tool until the upgrade is complete.

Step 14  Stop services on the A side Agent/IVR Controller.

Step 15  Upgrade the A side Agent/IVR Controller.

   • To perform a Common Ground upgrade, see Common Ground Upgrade (page 43)

   • To perform a Technology Refresh upgrade, see Technology Refresh Upgrade (page 44)

Step 16  Stop services on the B side Agent/IVR Controller.

Step 17  Start services on the A side Agent/IVR Controller.

   If A side operations fail, do not proceed further. Revert to the B side machines and troubleshoot A side operations before continuing with upgrade procedures.

Step 18  Upgrade the B side Agent/IVR Controller.

   • To perform a Common Ground upgrade, see Common Ground Upgrade (page 43)

   • To perform a Technology Refresh upgrade, see Technology Refresh Upgrade (page 44)

Step 19  Start services on the B side Agent/IVR Controller.

Step 20  Upgrade the following components in any order.

   • Outbound Controller (page 45)

   • Multichannel Controller (page 49)

   • CTI OS desktops (page 51)

   • CAD Server and Desktops (must be done together) (page 53)

   • Internet Script Editor
Upgrading Administration & WebView Reporting Machines and Central Controllers

You must upgrade Administration & WebView Reporting machines and Central Controller pairs (sides A and B) within the same maintenance window.

To fully understand the upgrade process, Cisco strongly suggests that you familiarize yourself with the high level overview of the upgrade process (page 35) in advance of performing the upgrade.

This chapter contains the following topics:

- **Common Ground Upgrade**, page 39
- **Technology Refresh Upgrade**, page 40

Common Ground Upgrade

You must perform the upgrade in an exact order, migrating one database at a time. In other words, in a duplexed environment you will need to repeat the following steps a total of four times beginning with the Administration & WebView Reporting machine whose preferred Central Controller is the side A Central Controller.

**Step 1** Be sure you have performed the pre-upgrade tasks (page 26).

**Step 2**

If: You are upgrading an Administration & WebView Reporting machine,

Then: Run EDMT (page 77) to migrate the HDS database (ipcc_hds).

If: If you are upgrading a Central Controller,

Then: Run EDMT (page 77) to migrate the Logger database (ipcc_side<A/B>).

**Step 3** From the installation media, run the Cisco IPCC Enterprise Installer (page 83) (setup.exe).
Step 4  Return to the step (within the High Level Overview of the Upgrade Process (page 35)) that referred you to this section.

Technology Refresh Upgrade

In the following procedure, we refer to the current 7.x machines as the source machines. New Unified SCCE 7.5 machines are referred to as the destination machines.

**Note:** The following procedure instructs you to upgrade Administration & WebView Reporting machines and Central Controller pairs. It is recommended that you reuse the IP address / machine name of the destination machine to match the IP address of the source Administration & WebView Reporting machine. At the time of publication, this is the supported course of action for a Technology Refresh upgrade because it minimizes downtime and reduces system reconfiguration.

**Caution:** To ensure a successful Unified SCCE upgrade, you MUST perform the upgrade procedure in the exact order.

**Step 1**  Be sure you have performed the pre-upgrade tasks (page 26).

**Step 2**  
If: You are upgrading an Administration & WebView Reporting machine,  
Then: Run EDMT (page 77) to migrate the HDS database (ipcc_hds).

If: If you are upgrading a Central Controller,  
Then: Run EDMT (page 77) to migrate the Logger database (ipcc_side<A/B>).

**Step 3**  Use the Microsoft SQL Backup and Restore utility to restore the backup version of WebView database on the destination Administration & WebView Reporting machine.

**Step 4**  Shut down or disconnect the corresponding source machine.

**Step 5**  From Active Directory Users and Computers on the domain controller, delete the source machine from the domain.

**Step 6**  On the destination machine, use Network Settings to change the IP address of the destination machine to match the IP address of the source machine.

**Step 7**  Navigate to System Properties > Computer Name and click Change to rename the machine to the name of source machine you deleted from the domain, and then join the machine to the domain.

**Note:** This practice helps to maximize system uptime and reduce system reconfiguration.

**Step 8**  Reboot the machine when prompted.

**Step 9**  From the installation media, run the Cisco IPCC Enterprise Installer (page 83) (setup.exe) on the destination machine.
You must run the Cisco IPCC Enterprise Installer on a local machine; it can not be run over the network.

**Step 10** Return to the step (within the *High Level Overview of the Upgrade Process (page 35)*) that referred you to this section.
Upgrading Agent/IVR Controllers

To fully understand the upgrade process, Cisco strongly suggests that you familiarize yourself with the high level overview of the upgrade process (page 35) in advance of performing the upgrade.

Note: If you intend to deploy the Outbound Controller on its own machine, it must be upgraded in the same maintenance window as the Agent/IVR Controller.

This chapter contains the following topics:

• Common Ground Upgrade, page 43
• Technology Refresh Upgrade, page 44

Common Ground Upgrade

Perform the following steps to do a Common Ground upgrade of an Agent/IVR Controller.

Step 1 Be sure you have performed the pre-upgrade tasks (page 26).

Step 2 From the installation media, run the Cisco IPCC Enterprise Installer (page 83) (setup.exe).

Step 3 Return to the step (within the High Level Overview of the Upgrade Process (page 35)) that referred you to this section.

Note: If you have upgraded Cisco Unified CM, you must upgrade the Cisco JTAPI client on the Agent/IVR Controllers. Refer to the Upgrade Guide Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.5(1) for instructions on how to install the JTAPI client from Cisco CallManager Administration.
Technology Refresh Upgrade

Caution: To ensure a successful upgrade, you MUST perform the upgrade procedure in exact order.

Perform the following steps to perform a Technology Refresh upgrade on the Agent/IVR Controller, sides A & B.

Step 1 Be sure you have performed the pre-upgrade tasks (page 26).

Step 2 Import the Cisco Systems, Inc. registry key—that you previously exported—from the matching source machine.

Step 3 Shut down or disconnect the source machine from the domain.

Step 4 From Active Directory Users and Computers on the domain controller, delete the source machine.

Step 5 Use Network Settings to change the IP address of the destination machine to match the IP address of the source Agent/IVR Controller.

Step 6 Navigate to System Properties > Computer Name and click Change to rename the machine to the name of the source machine you deleted from the domain. Join the machine to the domain.

Note:

- This practice helps to maximize system uptime and reduce system reconfiguration.

- If you have upgraded Cisco Unified CM, you must install the Cisco JTAPI client on the Agent/IVR Controllers before proceeding with the upgrade. Refer to the Upgrade Guide Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 7.5(1) for instructions on how to install the JTAPI client from Cisco CallManager Administration.

Step 7 Reboot the machine when prompted.

Step 8 From the installation media, run the Cisco IPCC Enterprise Installer (page 83) (setup.exe) on the destination Agent/IVR Controller.

Step 9 Return to the step (within the High Level Overview of the Upgrade Process (page 35)) that referred you to this section.
Upgrading the Outbound Controller

Note: If your Outbound Controller is deployed on its own machine and you intend to keep it as a standalone machine, you must upgrade it in the same maintenance window as the Agent/IVR Controller.

This chapter contains the following topics:

- Common Ground Upgrade, page 45
- Technology Refresh Upgrade, page 45
- Moving From a Standalone Outbound Controller, page 46

Common Ground Upgrade

For a Common Ground upgrade of Outbound Controller, do the following:

Step 1 Be sure you have performed the pre-upgrade tasks (page 26).

Step 2 From the installation media, run the Cisco IPCC Enterprise Installer (page 83) (setup.exe).

See Also

High Level Overview of the Upgrade Process (page 35)

Technology Refresh Upgrade

Perform the following steps to do a Technology Refresh upgrade on the Outbound Controller.

Step 1 Be sure you have performed the pre-upgrade tasks (page 26).

Step 2 Shut down or disconnect the source machine from the domain.
Step 3 From **Active Directory Users and Computers** on the domain controller, delete the source Outbound Controller.

Step 4 Use **Network Settings** to change the IP address of the destination machine to match the IP address of the source Outbound Controller.

**Note:** This practice helps to maximize system uptime and reduce system reconfiguration.

Step 5 Navigate to **System Properties** > **Computer Name** and click **Change** to rename the machine to the name of the source Outbound Controller you deleted from the domain. Join the machine to the domain.

Step 6 Reboot the machine when prompted.

Step 7 From the installation media, run the **Cisco IPCC Enterprise Installer (page 83)** (**setup.exe**) on the destination Outbound Controller.

Step 8 Upgrade the following components in any order.

- Multichannel Controller (page 49)
- CTI OS desktops (page 51)
- CAD Server and Desktops (page 53)(must be done together)

**See Also**

*High Level Overview of the Upgrade Process (page 35)*

**Moving From a Standalone Outbound Controller**

If you intend to co-locate your Outbound Controller on the Agent/IVR Controllers, you do not need to upgrade your standalone Outbound Controller.

Perform the following steps to move from a standalone Outbound Controller to an Outbound Controller that is co-located on the Agent/IVR Controller.

Step 1 Upon completion of the Unified SCCE upgrade, launch the Web Administration Tool and navigate to **System Management / Machine Management / Machines**.

Step 2 Delete the standalone Outbound Controller.

Step 3 Use the machine wizard to modify both Agent/IVR Controller machines and select the **with Outbound Controller** check box.

This action indicates a change in the machine's role.

Step 4 Verify Outbound functionality is working properly post-upgrade.
Chapter 7: Upgrading the Outbound Controller

Step 5  
Uninstall the standalone Outbound Controller machine.
Chapter 8

Upgrading the Multichannel Controller

Perform the following steps to upgrade the Multichannel Controller.

This chapter contains the following topics:

- Common Ground Upgrade, page 49
- Technology Refresh Upgrade, page 49

Common Ground Upgrade

Do the following for a Common Ground upgrade of the Multichannel Controller.

**Step 1** Be sure you have performed the pre-upgrade tasks (page 26).

**Step 2** From the installation media, run the Cisco IPCC Enterprise Installer (page 83) (setup.exe).

See Also

- Pre-Upgrade Tasks (page 26)
- High Level Overview of the Upgrade Process (page 35)
- Cisco IPCC Enterprise Installer (page 83)

Technology Refresh Upgrade

Perform the following steps to do a Technology Refresh upgrade on a Multichannel Controller.

**Step 1** Be sure you have performed the pre-upgrade tasks (page 26).

**Step 2** Shut down or disconnect the source machine from the domain.
Step 3  From Active Directory Users and Computers on the domain controller, delete the source Multichannel Controller.

Step 4  Use Network Settings to change the IP address of the destination machine to match the IP address of the source Multichannel Controller.

Note: This practice helps to maximize system uptime and reduce system reconfiguration.

Step 5  Navigate to System Properties > Computer Name and click Change to rename the machine to the name of the source Multichannel Controller you deleted from the domain. Join the machine to the domain.

Step 6  Reboot the machine when prompted.

Step 7  From the installation media, run the Cisco IPCC Enterprise Installer (page 83) (setup.exe) on the destination Multichannel Controller.

Step 8  Upgrade the following components in any order.

• Outbound Controller (page 45)

• CTI OS desktops (page 51)

• CAD Server and Desktops (page 53)(must be done together)

See Also

Pre-Upgrade Tasks (page 26)

High Level Overview of the Upgrade Process (page 35)

Cisco IPCC Enterprise Installer (page 83)
Chapter 9

Upgrading CTI OS Agent and Supervisor Desktop

Technology Refresh upgrades are no different than fresh installations, except that the original desktop is taken offline. Refer to the CTI OS System Manager’s Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted (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.

Common Ground Upgrade

Perform the following steps for a Common Ground upgrade of the standard CTI OS Agent and Supervisor Desktop.

- **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, and update configuration data as prompted.
- **Step 3** Reboot the machine if prompted.
Chapter 10

Upgrading Cisco Agent Desktop (CAD)

CAD 7.5 is integrated as follows:

Table 1:

<table>
<thead>
<tr>
<th>CAD Version</th>
<th>Unified CM Version</th>
<th>Unified SCCE Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5(1)</td>
<td>4.1, 4.2, 5.0, 6.0</td>
<td>7.5(1)</td>
</tr>
</tbody>
</table>

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.

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.

If you are upgrading to CAD 7.5 from CAD 6.0(2), you must perform the following steps.

Upgrading from CAD 6.0(2) to CAD 7.5(1)

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.

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.
Part 4: Post-Upgrade Tasks

This section discusses tasks that you must perform after upgrading Unified SCCE.
Performing Post-Upgrade Tasks

Validate the Upgrade

After performing the Unified SCCE upgrade, perform post upgrade tests to verify that the upgrade succeeded.

Note: It may be necessary to run additional tests as required due to the new Release 7.5 functionality.

System Integrity Tests

The remaining tests are performed to ensure proper functionality of all system components 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
  
  For example, check the following processes for:
  
  – RouterA router - all configuration data transferred from logger
  
  – LoggerA configlogger- completed initialization
  
  – Distributor updateaw - completed update and waiting work
  
  • 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
Validate the Upgrade

Validate Scripts

**Step 1** Open Script Editor.

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

**Step 3** Verify that all scripts are functioning properly. Make note of any scripts that are not operating properly after the upgrade, then compare these to the list generated prior to the upgrade.

Redundancy Testing

**Step 1** Using the Web Administration Tool, choose Service Management > Machine Management > Machines and stop each active PG service to ensure that the backup PG assumes an active state.

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

**Step 3** Verify that all Services are set to start automatically.

**Step 4** Restart services.

Review Log Files

It is recommended that you review and monitor log files to troubleshoot and monitor the health of a system.

**Step 1** Using the log file analysis tool of your choice, review log files.

See Log Files (page 90) for a complete list of log files.
Note: If you intend to perform a Common Ground upgrade, complete the Unified SCCE upgrade before upgrading SQL Server from SQL 2000 to SQL 2005.

The SQL Server 2005 security hardening option is presented during Unified SCCE installation. If you have upgraded SQL Server and want to take advantage of security hardening, you will need to apply security hardening settings manually. Refer to the *Security Best Practices Guide for Cisco ICM/Unified Contact Center Enterprise & Hosted, Release 7.5(1)* for more information about security hardening.

This chapter contains the following topics:

- Upgrading from SQL Server 2000 to SQL Server 2005 - Common Ground Upgrades Only, page 59
- Installing Microsoft SQL Server 2005, page 66

**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.
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 tools—"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.
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.
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.


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

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


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

  b. Following the instructions provided with the service pack, install it.
Installing Microsoft SQL Server 2005
Database Tasks

When migrating from an older ICM/System IPCC release to a newer Unified ICME/Unified SCCE release, you need to look up 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.

Determining the Size of the ICM Database

Using ICMDBA

To determine the size of an ICM database using ICMDBA perform the following steps.

**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** Open **ipcc_side<A/B>** and select **Properties** to see the database size.

Using SQL Server 2000

To determine the size of an ICM database using SQL Server Enterprise Manager perform the following steps.
Determining the Size of the ICM Database

**Step 1**  On a system that has Microsoft SQL Server 2000 installed, navigate to the SQL Server 2000 install directory (by default at C:\Program Files\Microsoft SQL Server\MSSQL\Install).

**Step 2**  On the SQL Server systems, launch **Start > Programs > Microsoft SQL Server > ISQL_w**.

**Step 3**  Enter the required database connection information:

- Make sure that the current system name is selected.
- Select **Use Standard Security**.
- Make sure the login id is sa or equivalent.
- Supply a password if required.

**Step 4**  Click **Connect**.

**Step 5**  The Microsoft ISQL_w application opens. Make sure the selected database in the DB: drop down is **master**.

**Step 6**  Select **File > Open from the Microsoft ISQL/w menu**.

**Step 7**  Enter EXECUTE sp_helpdb into the Query window and execute the script by clicking the green arrow or by selecting **Query > Execute** from the Microsoft ISQL/w menu.

**Step 8**  Note the value located in the db_size column for the ICM database.

**Step 9**  Exit the Microsoft ISQL/w program.

**Using SQL Server 2005**

To determine the size of an ICM database using SQL Server Management Studio, perform the following steps.

**Step 1**  On a system that has Microsoft SQL Server 2005 installed, launch **Start > Programs > SQL Server Management Studio**

If you are running SQL Server 2005 for the first time, the Connect to Server window displays. Accept the defaults, and click **Connect**.

The SQL Server Management Studio application opens.

**Step 2**  Select **Databases > <database name>**

where database name is:

- ipcc_side<A/B>
- ipcc_hds
The Database Properties window opens to the General page.

**Step 3** Under the **Database**, note the value located in the Database pane.

**Step 4** Exit the SQL Server Management Studio application.
Determining the Size of the ICM Database
Exporting and Importing the Cisco Systems Inc.
Registry Key

Use the Registry Editor to export the Cisco Systems, Inc registry on each source machine and then import on the destination machine.

**Caution:** Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should always make a backup copy of the registry files before editing the registry.

### Exporting the Registry

Perform the following steps to export the registry.

---

**Step 1**
Open the Registry Editor.

**Step 2**
Locate the `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.` key.

**Step 3**
On the **File** menu, click **Export**.

**Step 4**
In the **File name** box, enter a name for the registry file.

**Step 5**
In the **Export range** box, select **Selected branch**.

**Step 6**
Click **Save**.

The file is saved with a .reg extension.
Importing the Registry

In Windows Explorer, double-clicking a file with the .reg extension imports the file into the computer’s registry.

You can also perform the following steps to import the registry key.

**Step 1**
Open the Registry Editor.

**Step 2**
On the **File** menu, click **Import Registry File**.

**Step 3**
Locate the file you previously exported, click the file to select it, then click **Open**.

**Step 4**
Verify that the file has been imported by looking at the entries under HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.

**Step 5**
Click **Exit**.
Running the EDMT Wizard


Prior to running EDMT to perform a Common Ground upgrade, be sure you have backed up system critical data. For a complete list of the data that you must back up and restore, copy and paste, or export and import, see Perform Back Ups (page 24).

Common Ground Wizard Screens

**Note:** Prior to running EDMT set the *Maximum file size* for the data files on the source database to *Unrestricted growth*. Refer to Technology Refresh Upgrade (page 26) for additional information.

To perform a Common Ground upgrade, perform the following steps.

**Step 1** Run EDMT and click **Next**.

The EDMT wizard opens.

**Step 2** Select **Common Ground** and click **Next**.

The Database Connection screen displays.
Step 3 Provide the ICM/IPCC database name `<ipcc_hds/ipcc_side<A/B>>` and click Next.

The Migration Control dialog appears.

Step 4 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 displays.

Step 5 Click Yes in response to the prompt.

Caution: If the migration process is interrupted, data and schema corruption may occur leaving the database in an inconsistent state. In this situation, you will need to restore your database from backup. If it becomes necessary to terminate an in-progress migration, click Terminate Migration and Exit.

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

Step 6 When the migration is complete, click Exit to close EDMT.

Step 7 Continue with the Common Ground upgrade of the Administration & WebView Reporting Machine and Central Controller (page 39).

Refer to the Upgrade Guide Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 7.5(1) for detailed explanation about EDMT panel and field descriptions.
Technology Refresh Wizard Screens

**Note:** Prior to running EDMT set the *Maximum file size* for the data files on the source database to *Unrestricted growth*. Refer to Technology Refresh Upgrade (page 26) for additional information.

To perform a Technology Refresh upgrade, perform the following steps.

**Step 1** Run EDMT and click **Next**.

The EDMT wizard opens.

**Step 2** Select **Technology Refresh** and click **Next**.

The Source and Destination Database Connection screen displays.

![Source/Destination Database Connection Dialog](image)

**Step 3** Provide the following information:

a. the hostname or IP address of the server hosting the database (Logger or HDS).

b. the ICM/IPCC database name `<ipcc_hds/ipcc_side<A/B>` and click **Next**.

The Backup Connection and Destination Restore Location screen displays.
Step 4 Provide the following information:

a. the Windows share name on your network to which the database will be backed up

b. the Windows Share Password and click Next.

The Migration Control dialog appears.

Step 5 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.

Step 6 Click Yes in response to the prompt.

Caution: If the migration process is interrupted, data and schema corruption may occur leaving the database in an inconsistent state. In this situation, you will need to restore your database from backup. If it becomes necessary to terminate an in-progress migration, click Terminate Migration and Exit.

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

Step 7 When the migration is complete, click Exit to close EDMT.

Step 8 Continue with the Technology Refresh upgrade of the Administration & WebView Reporting machines and Central Controller (page 40).
Refer to the *Upgrade Guide Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 7.5(1)* for detailed explanation about EDMT panel and field descriptions.
System IPCC Enterprise Installer

Running the System IPCC Enterprise Installation Program

The InstallShield Wizard updates the installed version of System IPCC Enterprise to version 7.5(1). This installation cannot be rolled back.

There are slight differences between the upgrade procedures for Common Ground and Technology Refresh upgrades. However, upgrading is fairly straight forward and the differences between the two upgrades are noted in the procedures that follow.

**Caution: Running the System IPCC Enterprise Installer over the network is unsupported. You must either run the Installer from the installation media (DVD) or copy the Installer directory to the target machine and then run from the local machine. Various and miscellaneous errors can occur during installation over the network. It is also important to remember that Release 7.5(1) is a full installation and that there is no automated rollback.**

Common Ground Upgrade

To upgrade to Unified SCCE 7.5(1), perform the following steps.

---

**Step 1**

From the installation media, run the Cisco IPCC Enterprise Installer for system deployment of IPCC (`setup.exe`).

The System IPCC Enterprise splash screen and a Preparing Setup display, followed by the Welcome screen.

**Step 2**

On the Welcome screen, click **Next**.

**Note:** Certain machine types require Microsoft .NET Framework 3.5, which is the latest release of the .NET Framework and is required for the Unified SCCE upgrade. If the installer detects
an earlier version, you are prompted to install the latest version. Choose Yes in response to the prompt. Click OK to reboot the machine and then relaunch the Cisco IPCC Enterprise installer.

The Service Account Management screen displays for certain types of machines.

Figure 6: CG Service Account Management Screen

Step 3

If: The Service Account Management screen does not display,
Then: proceed to Step 4.

If: The Service Account Management screen displays,
Then: choose a service account management option:

a. Do Not Modify Service Accounts (default)

The service accounts are not recreated and Service Account Manager is not invoked.

b. Installer Creates Service Accounts

System IPCC upgrade invokes the Service Account Manager tool silently, without bringing up the Service Account Manager.

c. 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. When the tool is closed, Unified SCCE upgrade takes control and finishes the installation steps.
Note: Service Account Management (SAM) is standalone software used to create Windows service accounts for some, but not all, Unified SCCE components. Service Account Management is invoked by the Cisco IPCC Enterprise Installer when you choose to manipulate the default service account creation process. If, after upgrade, you want to modify the way you manage service accounts, you can choose to run SAM from IPCC Administration.

Refer to the Upgrade Guide Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 7.5(1) for detailed explanation about managing service accounts.

The Security Hardening screen displays.

**Step 4** Choose whether to update security hardening and click **Next**.

A Version Checking message displays.

**Step 5** Click **Yes** to upgrade to version 7.5(1).

**Step 6** If you are upgrading Administration & WebView Reporting machines and Central Controllers, you are prompted to back up your database. If you choose Yes, the Choose Destination Folder dialog box displays. Specify a directory where the backup will reside and click **OK**.

The IPCC Enterprise Installer uses a preshared key to set up Support Tools with Internet Protocol Security (IPSEC). This key must be the same key used for the remote Support Tools server.

**Step 7** If: The IPsec key is present, the installer upgrades the Support Tools Node Agent silently,

Then: proceed to the next step.

If: The IPsec key is not present, the installer prompts you to enter a Preshared Key

Then: enter a Preshared Key and click **Next**.

The preshared key can be any non-null string of any combination of up to 256 Unicode characters. When specifying a key, be mindful of your users. A key that is long and complex may provide adequate security, but might be difficult for your users to type accurately.

Valid characters for the Preshared Key are:

- Alphanumeric characters

- Space

- Any of the following special characters: -,.#&/~!@$%^*()+={}\[<>?;:_

**Step 8** In the IPCC Machine Initializer dialog, it is imperative that you keep the existing facility as the source machine. You must accept the facility that displays in the Facility drop-down list, and click **OK**.
Step 9  

On the Upgrade Complete screen, choose whether to restart the machine and click **Finish**.

Refer to the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 7.5(1)* for detailed explanation about using Service Account Management to manage service accounts.

**Technology Refresh Upgrade**

**Step 1**  

From the installation media, run the Cisco IPCC Enterprise Installer for system deployment of IPCC (*setup.exe*).

The System IPCC Enterprise splash screen and a Preparing Setup display, followed by the Welcome screen.

**Step 2**  

On the Welcome screen, click **Next**.

**Note:** Certain machine types require Microsoft .NET Framework 3.5, which is the latest release of the .NET Framework and is required for the Unified SCCE upgrade. If the installer detects an earlier version, you are prompted to install the latest version. Choose **Yes** in response to the prompt. Click **OK** to reboot the machine and then relaunch the Cisco IPCC Enterprise installer.

The Service Account Management screen displays for certain types of machines.
Step 3

If: The Service Account Management screen does not display,

Then: proceed to Step 4.

If: The Service Account Management screen displays,

Then: choose a service account management option:

a. Installer Creates Service Accounts

Unified SCCE upgrade invokes the Service Account Manager tool silently, without bringing up the Service Account Manager.

b. 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. When the tool is closed, Unified SCCE upgrade takes control and finishes the installation steps.

Note: Service Account Management (SAM) is standalone software used to create Windows service accounts for some, but not all, Unified SCCE components. Service Account Management is invoked by the Cisco IPCC Enterprise Installer when you choose to manipulate the default service account creation process. If, after upgrade, you want to modify the way you manage service accounts, you can choose to run SAM from IPCC Administration.

Refer to the Upgrade Guide Cisco Unified ICM/Contact Center Enterprise & Hosted Release 7.5(1) for detailed explanation about managing service accounts.
The Security Hardening screen displays.

**Step 4**

Choose whether to update security hardening and click **Next**.

The installer begins verifying the IPSec configuration. When this process is complete, the Configure Support Tools screen displays.

The IPCC Enterprise Installer uses a Preshared Key to set up Support Tools with Internet Protocol Security (IPSEC). This key must be the same key used for the remote Support Tools server.

**Step 5**

**If:** The IPSec key is present, the installer upgrades the Support Tools Node Agent silently,

**Then:** proceed to the next step.

**If:** The IPSec key is not present, the installer prompts you to enter a Preshared Key

**Then:** enter a preshared Key and click **Next**.

The preshared key can be any non-null string of any combination of up to 256 Unicode characters. When specifying a key, be mindful of your users. A key that is long and complex may provide adequate security, but might be difficult for your users to type accurately.

Valid characters for the Preshared Key are:

- Alphanumeric characters
- Space
- Any of the following special characters: -,.@'!+$%^*()+={}\<;:_

The Start Copying Files screen displays.

**Step 6**

Click **Back** to review or change settings, click **Next** to begin copying files.

The Setup Status screen displays a progress bar while Cisco IPCC Enterprise Installer configures your new installation. When complete, the IPCC Machine Initializer screen displays.
Figure 9: IPCC Machine Initialization Screen

In the IPCC Machine Initializer dialog, it is imperative that you keep the existing facility as the source machine. You must accept the facility that displays in the Facility drop-down list, and click OK.

When machine initialization is completed, you are prompted to confirm your choice, click OK.

Note: You must accept the defaults on the IPCC Machine Initializer screen. The ability to change a facility is not currently supported. This feature will be supported in a future release.

Step 8
On the Upgrade Complete screen, choose whether to restart the machine and click Finish.

Enabling the Transport Layer Security (TLS) 1.0 Protocol

In release 7.2(1) or later, Operating System security hardening settings on Windows Server 2003 secure the IIS webserver by default. Specifically, the security template enables FIPS compliant strong encryption, which requires the Transport Layer Security (TLS) 1.0 protocol be enabled instead of SSL 2.0 or SSL 3.0. TLS 1.0 is enabled on Internet Explorer 7.0 by default, but is not enabled on Internet Explorer 6.0. To ensure Web browser connectivity to a hardened Webview, Agent Reskilling, or Unified SCCB Webconfig server over HTTPS using Internet Explorer 6, you need to enable TLS 1.0 protocol.

Enabling the TLS 1.0 Protocol

Perform the following steps to enable the TLS 1.0 protocol.

Step 1
Launch Internet Explorer 6.0.
Step 2  On the Tools menu, click Internet Options.

Step 3  Select the Advanced tab.

Step 4  Scroll to Security and select the Use TLS 1.0 checkbox.

Be sure to consult the Microsoft Knowledge Base (KB) KB811833 (http://support.microsoft.com/kb/811833) for additional information about security settings.

Note: If security hardening is applied using the 7.2(1) or later template but Internet Explorer is not configured to support the TLS 1.0 protocol, the Web browser will not be unable to connect to the Web server. An error message indicates that the page is either unavailable or that the Web site might be experiencing technical difficulties.

Locating Log Files

The Cisco IPCC Enterprise installer maintains three log files.

Here is a list of log file locations.

- The System IPCC Installer log files are named IPCCInstall.log and are located in:
  c:\temp\IPCCInstallLogs in date- and time-stamped directories.

- IPCC Machine Initializer log files are found in c:\temp\IpccMachineInitialization.log. When launched by the Installer, tracing and error messages are in the installation log file under: c:\temp\IPCCInstallLogs.

- Service Account Manager Log file is found in c:\temp\ServiceAccountManager.log.

Note: IPCC Machine Initializer and Service Account Manager logs are included in the Installer log file when they are launched by the Installer.

You can also view third party software logs.

Here is a list of third party log file locations.

- EAServer
  c:\temp\ES Server<version>.log

- New Atlanta Servlet Exec
  c:\temp\NA SEI.log<version>

- PowerBuilder
  c:\temp\pbvm 10 install.log
- WebView Third Party
  c:\temp\WV Third Party Installer.log

- Java
  c:\temp\JDK<version> setup.log

Refer to the *Installation and Configuration Guide Cisco Unified System Contact Center Enterprise 7.5(1)* for detailed information about Unified SCCE troubleshooting.
Uninstalling Unified SCCE

If you have installed Unified SCCE but have not deployed your newly installed system, you can simply uninstall.

The System IPCC Enterprise uninstall feature is supported with Microsoft's Add and Remove Programs tool. You must use this tool to perform a full uninstall of Unified SCCE 7.5; the System IPCC Enterprise installer cannot be used to uninstall Unified SCCE.

**Note:** Uninstall does not remove the databases, Internet Script Editor, or CTI OS programs.

The Unified SCCE 7.5 upgrade cannot be rolled back to a previous version.

**Caution:** Running the System IPCC 7.5 Enterprise installer a second time puts you into an upgrade mode in which uninstalling is NOT an option.

Uninstalling a Unified SCCE 7.5 Installation

**Step 1** Perform the following steps to uninstall an active system:

1. Launch the ICM/IPCC Web Administration tool and navigate to **System Management > Machines Management > Machines**, then locate the machine and remove it from your deployment.

2. Open **Add or Remove Programs** tool and click Change or Remove Programs, then click remove.

**Step 2** Perform the following steps to uninstall a system that you have not deployed:

- Open **Add or Remove Programs** tool and click **Change or Remove Programs**, then click **Remove**.
Uninstalling Unified SCCE
# Index

<table>
<thead>
<tr>
<th>Category</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>18</td>
</tr>
<tr>
<td>Administration and WebView reporting machines</td>
<td>32</td>
</tr>
<tr>
<td>Agent/IVR Controllers</td>
<td>32</td>
</tr>
<tr>
<td>Apache Tomcat</td>
<td>17</td>
</tr>
<tr>
<td>back ups</td>
<td>24, 10</td>
</tr>
<tr>
<td>CAD desktops</td>
<td>53</td>
</tr>
<tr>
<td>Central Controllers</td>
<td>32</td>
</tr>
<tr>
<td>Cisco notifications</td>
<td>13, 13, 13</td>
</tr>
<tr>
<td>Cisco Security Agent (CSA)</td>
<td>18</td>
</tr>
<tr>
<td>Common Ground method</td>
<td>11</td>
</tr>
<tr>
<td>CTI desktops</td>
<td>51</td>
</tr>
<tr>
<td>CTI Server version</td>
<td>17</td>
</tr>
<tr>
<td>database tasks</td>
<td>71</td>
</tr>
<tr>
<td>EDMT Wizard</td>
<td>77, 79</td>
</tr>
<tr>
<td>EDMT Wizard enhancements</td>
<td>2</td>
</tr>
<tr>
<td>FIPS compliant encryption</td>
<td>89</td>
</tr>
<tr>
<td>FIPS compliant encryption with TLS 1.0 Protocol</td>
<td>89</td>
</tr>
<tr>
<td>ICMDBA</td>
<td>71</td>
</tr>
<tr>
<td>ICMDBA sizing with</td>
<td>71</td>
</tr>
<tr>
<td>installer for Unified SCCE</td>
<td>15, 83, 17</td>
</tr>
<tr>
<td>Installers running</td>
<td>83</td>
</tr>
<tr>
<td>third-party software</td>
<td>17</td>
</tr>
<tr>
<td>IVR functionality</td>
<td>32</td>
</tr>
<tr>
<td>JDK/SDK</td>
<td>17</td>
</tr>
<tr>
<td>location</td>
<td>16</td>
</tr>
<tr>
<td>log files</td>
<td>90</td>
</tr>
<tr>
<td>SQL Server backup of databases with EDMT</td>
<td>26, 77</td>
</tr>
<tr>
<td>compatibility component versions</td>
<td>14</td>
</tr>
<tr>
<td>components compatibility</td>
<td>14</td>
</tr>
<tr>
<td>CTI OS desktops</td>
<td>51</td>
</tr>
<tr>
<td>CTI OS Server version</td>
<td>17</td>
</tr>
<tr>
<td>database tasks sizing the ICM database</td>
<td>71</td>
</tr>
<tr>
<td>using ICMDBA program</td>
<td>71</td>
</tr>
<tr>
<td>using Microsoft ISQL_w program</td>
<td>71</td>
</tr>
<tr>
<td>disk space needed for migration</td>
<td>22</td>
</tr>
<tr>
<td>EDMT Wizard Common Ground</td>
<td>77</td>
</tr>
<tr>
<td>EDMT Wizard Technology Refresh</td>
<td>79</td>
</tr>
<tr>
<td>Enhanced Data Migration Tool see EDMT</td>
<td>77</td>
</tr>
<tr>
<td>EDMT Wizard enhancements collocation of Outbound Controller</td>
<td>2</td>
</tr>
<tr>
<td>integration with Unified CVP</td>
<td>2</td>
</tr>
<tr>
<td>FIPS compliant encryption with TLS 1.0 Protocol</td>
<td>89</td>
</tr>
<tr>
<td>ICMDBA sizing with</td>
<td>71</td>
</tr>
<tr>
<td>installer for Unified SCCE built-in upgrade functionality</td>
<td>15</td>
</tr>
<tr>
<td>running</td>
<td>83</td>
</tr>
<tr>
<td>third-party software</td>
<td>17</td>
</tr>
<tr>
<td>IVR functionality</td>
<td>32</td>
</tr>
<tr>
<td>JDK/SDK version</td>
<td>17</td>
</tr>
<tr>
<td>localization</td>
<td>16</td>
</tr>
<tr>
<td>log files installer</td>
<td>90</td>
</tr>
</tbody>
</table>
IPCC Machine Initializer...90
locating...90
review after upgrade...58
Service Account Manager...90
third-party software...90
machines
removing from your deployment...93
methods of upgrade
Common Ground...11
Technology Refresh...11
Microsoft .NET framework
version...17
Microsoft ISQL_w program
on SQL Server...71
Multichannel Controller
Common Ground upgrade...49
Technology Refresh upgrade...49
network
inventory...12
route plan...13
Outbound Controller...33
Common Ground upgrade...45
moving from standalone...46
Technology Refresh upgrade...45
plans
back up...10
hardware requirements...14
network route plan...13
post-upgrade test...10
pre-upgrade test...10
software requirements...14
post-upgrade tasks...55
redundancy tests...58
review of log files...58
system integrity tests...57
validate scripts...58
preparing to upgrade
back-up plan...9
default network route plan...9
defined upgrade steps...9
methods...9
network inventory...9
pre-upgrade tasks...19
schedule of activities...9
server preparation...21
software needed...10
test plans...9
what you need...9
pre-upgrade tasks
Common Ground ...26
configuring tempdb log files...22
performing back ups...24
performing system integrity test...24
preparing the servers...21
Technology Refresh...26
verifying disk space...22
redundancy tests...58
Registry Editor
exporting Cisco registry key...75
registry key
exporting with Registry Editor...75
importing with Registry Editor...76
registry settings...16
requirements
hardware and software...14
service or maintenance release...15
schedule
associated personnel...12
scripts
validating...58
Windows firewall configuration...14
security hardening
  for SQL Server...59
  Security Wizard...16
Security Wizard
  installs security settings...16
sizing the ICM database
  using ICMDBA...71
  using SQL Server 2000...71
  using SQL Server 2005...72
SQL Server
  database tasks...59
  Microsoft ISQL_w program...71
    supported versions...18
steps required...13
Support Tools
  version...17
system integrity tests
  performing...24
Technology Refresh method...11
  for Administration and WebView reporting machines...40
  for Agent/IVR Controllers...44
  for Central Controllers...40
  for Multichannel Controller...49
  for Outbound Controller...45
  for Unified SCCE...86
  network inventory...12
  pre-upgrade steps...26
    with EDMT...79
TempDB log
  autogrow with SQL Server 2000...22
  autogrow with SQL Server 2005...23
third-party installers
  Apache Tomcat...17
  CTI OS Server...17
in Unified SCCE installer...17
JDK/SDK...17
Microsoft .NET framework...17
Support Tools...17
WebView third-party tools...17
TLS 1.0 Protocol
  enabling...89
  FIPS compliant encryption...89
Transport Layer Security
  see TLS...89
uninstalling
  Unified SCCE...93
upgrading
  about Unified SCCE upgrade...31
  Administration and WebView reporting machines...31
  Agent/IVR Controllers...32
  CAD desktops...53
  Central Controllers...31
  CTI OS desktops...51
  Outbound Controller...33
  process overview...35
  validation
    after upgrade...57
  Web Administration Tool
    launching...93
  WebView third-party tools...17