Upgrading Contact Center Software Components

This topic discusses in more detail the upgrade sequence for all the contact center components configured in specific deployment models for Cisco Unified Communications Release 5.0.

Upgrade procedures for individual components are not described in this document, since they are available in individual component upgrade documents. See the Related Documentation section at the end of this topic for the appropriate upgrade documents and their URLs.

This topic contains the following sections:

- Contact Center Deployment Models
- Upgrading Contact Center Components
- Related Documentation

Contact Center Deployment Models

Upgrade procedures in this document are specifically tailored for each of the deployment models in the contact center test environment, since each of the sites includes different components.

Detailed information about these contact center deployment models at the different sites is available in the *System Architecture Reference Manual for Contact Center* at: http://www.cisco.com/univercd/cc/td/doc/systems/unified/unified1/starmipc/ch2model.htm

Listed below are the various deployment models in the Cisco Unified Communications contact center test environment:

- Single Site
- Multi-Site Centralized
- Multi-Site Distributed

Compare the above deployments to your specific deployment to best understand the upgrade process that is applicable in your environment.

This section provides the general upgrade sequence for the various components in the different deployment models. More detailed upgrade procedures are discussed later in this topic.

Single Site

In the contact center single site model, upgrade the components in the following order:

1. Infrastructure components including Catalyst 6K switches, routers, and domain controllers (including Active Directory)
2. Contact center components:
   a. Real-time Administration Workstation (at least one)
   b. ICM Progger (combination Peripheral Gateway, Router, Logger, CTI OS and CAD servers)
   c. Customer Voice Portal Voice Browser/ Application Server/ HTTP Media Server
   d. Cisco Outbound Option Dialer
   e. CTI OS Agent and Supervisor Desktop
   f. Cisco Agent Desktop (CAD) and Cisco Supervisor Desktop (CSD)
   g. VoIP Monitor
3. Windows Operating System
4. CRS (IP IVR)
5. Cisco CallManager servers (Cisco IP Phones are upgraded at the same time)
6. PSTN Gateways
7. Cisco applications co-resident on MCS servers (such as Cisco Security Agent, JTAPI software, etc.)
8. Third-party applications co-resident on MCS servers (Antivirus, Backup agent, Management agent (SNMP), etc.)

Note For Unified CallManager Release 5.0(2), co-residency of third-party applications is not supported.

9. Cisco and third-party adjunct applications or endpoints on other servers

Multi-Site Centralized

In the contact center multi-site centralized model, upgrade the components in the following order:

1. Infrastructure components including Catalyst 6K switches, routers, and domain controllers (including Active Directory)
2. Contact center components:
   a. Real-time Administration Workstation (at least one)
   b. ICM Rogger (combination Router and Logger)
   c. Peripheral Gateway
   d. CTI OS Server
   e. CAD Server
   f. Customer Voice Portal Voice Browser/ Application Server/ HTTP Media Server
   g. Cisco Outbound Option Dialer
   h. CTI OS Agent and Supervisor Desktop

    i. Cisco Agent Desktop (CAD) and Cisco Supervisor Desktop (CSD)
    j. VoIP Monitor

3. Windows Operating System
4. CRS (IP IVR)
5. Cisco CallManager servers (Cisco IP Phones are upgraded at the same time)
6. PSTN Gateways
7. Cisco applications co-resident on MCS servers (such as Cisco Security Agents, JTAPI software, etc.)
8. Third-party applications co-resident on MCS servers (Antivirus, Backup agent, Management agent (SNMP), etc.)

Note For Unified CallManager Release 5.0(2), co-residency of third-party applications is not supported.

9. Cisco and third-party adjunct applications or endpoints on other servers

Multi-Site Distributed

In the contact center multi-site distributed model, upgrade the components in the following order:

1. Infrastructure components including Catalyst 6K switches, routers, and domain controllers (including Active Directory)
2. Contact center components:
    a. Real-time Administration Workstation (at least one)
    b. ICM Rogger
    c. Peripheral Gateway
    d. CTI OS Server
    e. CAD Server
    f. Customer Voice Portal Voice Browser/ Application Server/ HTTP Media Server
    g. Cisco Outbound Option Dialer
    h. CTI OS Agent and Supervisor Desktop
    i. Cisco Agent Desktop (CAD) and Cisco Supervisor Desktop (CSD)
    j. VoIP Monitor
3. Windows Operating System
4. CRS (IP IVR)
5. Cisco CallManager servers (Cisco IP Phones are upgraded at the same time)
6. PSTN Gateways
7. Cisco applications co-resident on MCS servers (such as Cisco Security Agent, JTAPI software, etc.)
8. Third-party applications co-resident on MCS servers (Antivirus, Backup agent, Management agent (SNMP), etc.)

Note For Unified CallManager Release 5.0(2), co-residency of third-party applications is not supported.

9. Cisco and third-party adjunct applications or endpoints on other servers

Upgrading Contact Center Components

This section describes the following upgrade strategies for contact center components:

- Single Stage Upgrade—Recommended for small single/multi-site installations.
- Multi-Staged System Upgrade—Recommended for medium/large single-site and medium multi-site installations.
- Multi-Site Migration—To upgrade large, multi-site contact center installations to the Cisco Unified Communications release set using the Multi-Site Migration upgrade strategy, you can use either the Single Stage or Multi-Staged System upgrade procedures listed in this section.

See "Planning Your System Upgrade" for detailed information on the above upgrade strategies and Chapter 2, "Preparing for System Upgrade" for the software release versions of the components involved in the upgrade. For more information about the number of seats in these various types of sites, see the Summary of Upgrade Strategies table in "Planning Your System Upgrade."

Single Stage Upgrade

The Single Stage upgrade process is recommended for small single/multi-site installations and can be performed in a single maintenance window. This enables you to upgrade all the components in a brief period of time with no loss of functionality.

You should upgrade the components in the order listed in Table 4-1:

Table 4-1 Single Stage Upgrade Order for Contact Center Components

Order of Upgrade	Components being Upgraded
1	Cisco Catalyst 6500 + MSFC/SUP2 (core switch)
2	Cisco Catalyst 6500 + SUP2 (access switch)
3	Domain Controllers (including Active Directory)
4	Real Time AW/HDS/Webview
5	ICM Rogger
6	Peripheral Gateway
7	CTI OS Server
8	CAD Server
9	Customer Voice Portal Voice Browser/Application Server/HTTP Media Server
10	Cisco Outbound Option Dialer
11	CTI OS Agent & Supervisor Desktop
12	CAD Agent & Supervisor Desktop

Table 4-1 Single Stage Upgrade Order for Contact Center Components (continued)

Order of Upgrade	Components being Upgraded
13	Windows Operating System
14	CRS (IP IVR)
15	Cisco CallManager cluster (Cisco IP Phones are upgraded along with the cluster)
16	Voice and Data Gateways

Multi-Staged System Upgrade

A Multi-Staged System upgrade is the recommended approach for medium/large single-site and medium multi-site installations. In this upgrade process, components are grouped together for upgrading in several stages or maintenance windows. Within each maintenance window, there is a recommended order for upgrading each component.

The grouping of the components into the stages may vary depending on the size of the networks being upgraded. For smaller networks, one or more separate maintenance windows may be collapsed into a single maintenance window. Additional stages may be necessary for larger sites.

After each maintenance window, we recommend that you verify that the operation of all basic and critical call types remains unaffected, before you initiate the next upgrade stage listed in the table.

See Chapter 2, "Preparing for System Upgrade" for the software release versions of the components involved in the upgrade.

The stages and the contact center components you should upgrade during each stage are listed in Table 4-2.

Table 4-2 Multi-Staged System Upgrade Order for Contact Center Components

Stage	Component Groupings	Upgrade Order of Components in Each Stage
1	Switches and Domain Controllers	1. Core Switch 2. Access Switch 3. Domain Controllers (including Active Directory)
2	ICM Roggers and Real Time AW/HDS/Webview	1. Real Time AW/HDS/Webview 2. ICM Rogger
3	Peripheral Gateway, CTI OS and CAD servers, Cisco Outbound Option, and Customer Voice Portal components	1. Peripheral Gateway 2. CTI OS Server 3. CAD Server 4. Customer Voice Portal Voice Browser/ Application Server/ HTTP Media Server 5. Cisco Outbound Option Dialer
4	CTI OS/CAD Agent and Supervisor Desktop clients	1. CTI OS Agent/Supervisor Desktop 2. CAD Agent/Supervisor Desktop
5	Windows Operating System	1. Windows 2000 to Windows 2003

Table 4-2 Multi-Staged System Upgrade Order for Contact Center Components (continued)

Stage	Component Groupings	Upgrade Order of Components in Each Stage
6	CRS (IP IVR) and Cisco CallManager cluster (Cisco IP Phones are upgraded along with the cluster)	1. CRS (IP IVR) 2. Cisco CallManager cluster (Cisco IP Phones are upgraded along with the cluster)
7	Voice and Data Gateways	1. IOS Gateways (MGCP) 2. IOS Gateways (H.323) 3. Cisco CVP VXML Gateways 4. Cisco Gatekeepers

Upgrading a Specific Contact Center Test Bed

The contact center test sites are set up as two separate test beds:

- Test Bed 1—IP IVR test bed with Unified CallManager Post-Routed call flows. In Test Bed 1, the parent and child model has been implemented as part of Cisco Unified Communications system testing.
- Test Bed 2—CVP test bed with Unified CVP Post-Routed call flows

Test Bed 1: Cisco Unified CallManager Post-Routed and Parent/Child Call Flows

Use the flow chart shown in Figure 4-1 to determine the various installation and upgrade options that are available based on the type of call flow that is being implemented in your environment:

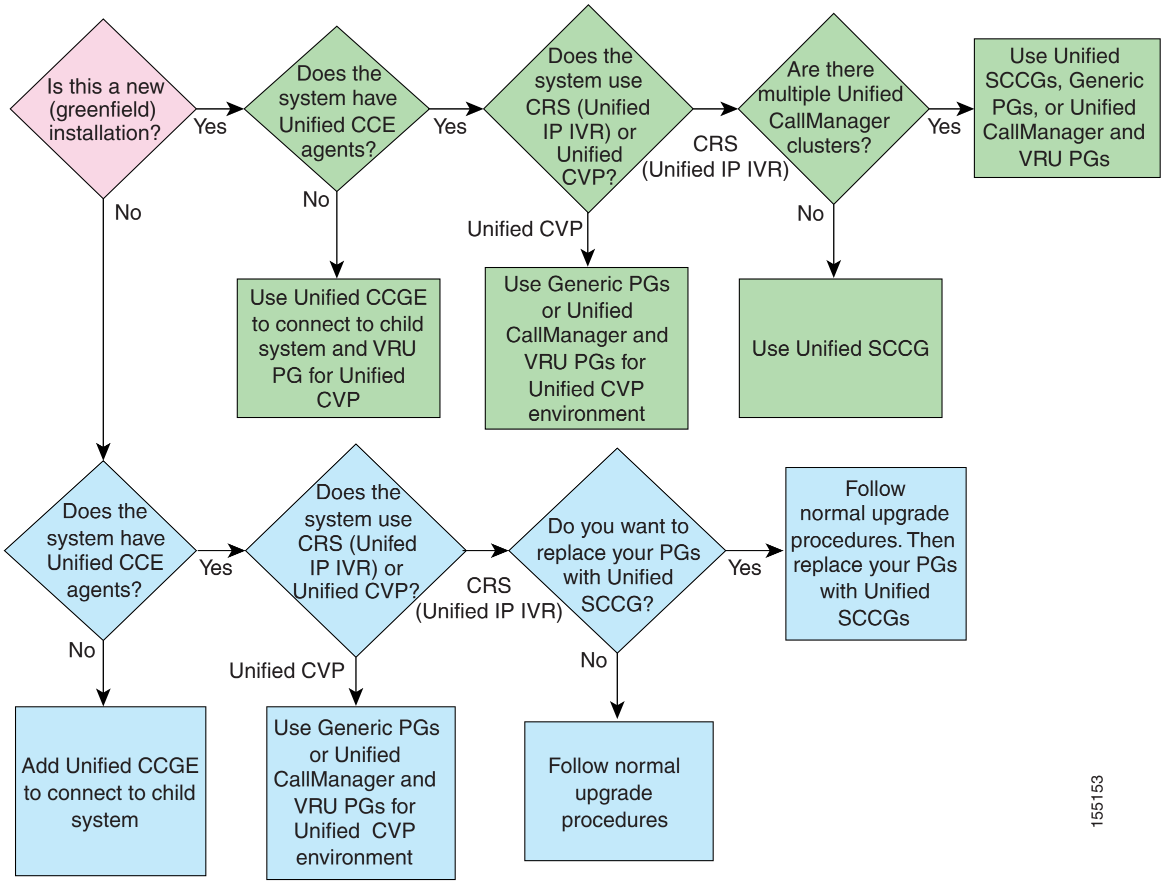
- Traditional Unified CallManager Post-Routed call flows where you can use normal upgrade procedures based on the single staged or multi-staged upgrade approaches discussed in Chapter 1, “Planning Your System Upgrade”
- New Parent/Child call flows (where Unified SCCG and Unified CCGE components must be newly installed and configured using Unified SCC streamlined installation and web-administration)

Note For the new parent and child model, there is no upgrade path. The deployment has to be treated as a “fresh installation.”

For detailed information on the deployment options and limitations for the Unified CallManager Post-Routed and Parent/Child call flows, see the Cisco Unified Contact Center Gateway feature in the the *System Architecture Reference Manual for Contact Center* at: http://www.cisco.com/univercd/cc/td/doc/systems/unified/unified1/starmipc/ch2model.htm

For information on related installation and upgrade considerations, see Cisco Intelligent Contact Management Considerations.

Figure 4-1 Installation and Upgrade Options in Test Bed 1


Is this a new (greenfield) installation?
Yes
No
Does the system have Unified CCE agents?
Yes
No
Does the system use CRS (Unified IP IVR) or Unified CVP?
CRS (Unified IP IVR)
Unified CVP
Are there multiple Unified CallManager clusters?
Yes
No
Use Unified SCCGs, Generic PGs, or Unified CallManager and VRU PGs
Use Unified CCGE to connect to child system and VRU PG for Unified CVP
Use Generic PGs or Unified CallManager and VRU PGs for Unified CVP environment
Use Unified SCCG
Does the system have Unified CCE agents?
Yes
No
Does the system use CRS (Unifed IP IVR) or Unified CVP?
CRS (Unified IP IVR)
Unified CVP
Do you want to replace your PGs with Unified SCCG?
Yes
No
Follow normal upgrade procedures. Then replace your PGs with Unified SCCGs
Add Unified CCGE to connect to child system
Use Generic PGs or Unified CallManager and VRU PGs for Unified CVP environment
Follow normal upgrade procedures
155153

For detailed installation and upgrade information on the Unified SCCG and Unified CCGE, see *Cisco IPCC Gateway Deployment Guide ICM/IPCC Enterprise Edition Release 7.0(0)* at:

http://www.cisco.com/application/pdf/en/us/guest/products/ps1001/c1097/ccmigration_09186a0080626383.pdf

For detailed information on the streamlined installation and web-based administration of the Unified SCC, see *System IPCC Enterprise Installation and Configuration Guide, Cisco IPCC Enterprise Edition* at:

http://www.cisco.com/application/pdf/en/us/guest/products/ps1844/c1676/ccmigration_09186a00804d8b1c.pdf

Test Bed 2: Cisco Unified Customer Voice Portal Post-Routed Call Flows

This section describes the detailed upgrade procedures for the components in Test Bed 2 using the Multi-Staged System upgrade approach. Individual contact center components are upgraded from the 4.1 release set to Cisco Unified Communications release software during separate maintenance windows.

Note To verify the interoperability between clusters running the previous and target release versions, some of the Cisco CallManager clusters in Test Bed 2 are not upgraded.

The different stages and the order of components within each stage are listed in Table 4-2. The following is a sequential list of the tasks required to upgrade the contact center components in Test Bed 2:

1. Verify software versions of components being upgraded.
2. Set up the new Active Directory environment prior to upgrading components.
3. Upgrade the existing ICM Support Tools Server to ensure compatibility with the Support Tools Agents.
4. Upgrade the core and access switches.
5. Upgrade the Distributor AW/HDS after performing a full system backup.
6. Upgrade the Side A ICM Central Controller components.
7. Upgrade the Side B ICM Central Controller components.
8. Upgrade the client Administration Workstation (AW).
9. Upgrade the Peripheral Gateway (Side A and Side B) and associated CTI servers, CTI OS servers, and Cisco Outbound Option Dialers.
10. Upgrade CTI OS Agent and Supervisor Desktop.
11. Upgrade from Windows 2000 to Windows Server 2003.
12. Upgrade Cisco CallManager clusters.
13. Upgrade Gateways and Gatekeepers.

Verify Software Versions

Ensure that the contact center components targeted for the upgrade are at the current release versions. See the Upgrade Release Versions table for contact center components in Chapter 2, “Preparing for System Upgrade” for the correct software versions.

Set up New Active Directory Environment

Set up the new Active Directory (AD) environment *prior* to starting the upgrade process to ensure proper interworking with Cisco Unified Intelligent Contact Management (Unified ICM) Release 7.0. Make sure of the following:

- Loggers are no longer domain controllers
- You set the Active Directory mode in Windows to the native mode. If not, the ICM system fails to create the necessary user accounts and groups in the domain.

The ICM Setup can detect the mode the domain is set at via the Domain Manager tool. If it detects that the Active Directory in Windows is not set up correctly (that is, in native mode), the ICM Setup prevents users from installing the ICM system.

Set up the new Active Directory (AD) environment as follows:

1. Upgrade existing AD domain controllers to Windows Server 2003.
2. Raise the Domain and Forest functionality to Windows Server 2003.

For information on upgrading Windows 2000 domain controllers to Windows Server 2003, see *How to upgrade Windows 2000 domain controllers to Windows Server 2003* on the Microsoft Help and Support website.

Upgrade Existing Intelligent Contact Management Support Tools Server

Upgrade the existing ICM Support Tools Server to ensure compatibility with the newer Support Tools Agents installed on the ICM nodes during the upgrade process. The ICM Support Tools Server is compatible with the older Support Tools Agents.

Upgrade Core and Access Switches

1. Copy the correct image on each switch via TFTP.
2. Modify the boot system configuration to enable loading of the new image.
3. Reboot the switch. The switch reads the modified configuration and reloads with the new image.

Upgrade Distributor Administrator Workstation/Historical Database Server

1. Using ICM Service Control, stop all ICM services on the AW/HDS.
2. Using ICM Service Control, change all ICM services on the AW/HDS to Manual Restart.
3. Perform a full system backup of the AW/HDS so that it can be restored in case a critical failure occurs.
4. Uninstall the Cisco Security Agent and the ICM Policy.
5. Upgrade third-party software such as virus protection software and VNC or PC Anywhere.
6. Reboot the AW/HDS.
7. Install the ICM Support Tools Agent. It is not necessary to uninstall older versions of the Support Tools Agent.
8. Use the ICM Third Party Tools CD and upgrade the JDK, ServletExec, and EA Server.
9. Use the data migration tool (EDMT) to update the HDS database.
10. Using the Domain Manager, add the AW/HDS instance to the appropriate Active Directory Instance Organizational Unit.
11. Run ICM *setup.exe* from the ICM Software CD on the AW/HDS. When the main setup screen appears, click Upgrade All.
12. Reboot the AW/HDS.
13. Install the latest Service Release and any required Engineering Specials on the AW/HDS.
14. Install Cisco Security Agent with ICM Policy on the AW/HDS.

Upgrade Side A Central Controller Components

1. Disable configuration changes by setting the *HKEY_LOCAL_MACHINE\ Software\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\ CurrentVersion\Configuration\Global\DBMaintenance* key to "1" on both Side A and Side B routers of the system being upgraded.

Note When disabling configuration settings on the Side B router, substitute 'RouterA' with 'RouterB' in the preceding registry key information.

2. Verify that you can no longer make configuration changes. The following message should display when attempting to save a configuration change: *Failed to update the database. Exclusive access to the router denied because configuration changes are currently disabled in the router registry.*
3. Using ICM Service Control, stop all ICM services on the Side A Rogger (Central Controller).
4. Using ICM Service Control, change all ICM services on the Side A Rogger to Manual Restart.
5. Perform a full system backup of the Side A Rogger so that it can be restored in case a critical failure occurs.
6. Uninstall the Cisco Security Agent and the ICM Policy.
7. Upgrade third-party software such as virus protection software and VNC or PC Anywhere.
8. Reboot the Side A ICM Rogger.
9. Install the ICM Support Tools Agent. It is not necessary to uninstall older versions of the Support Tools Agent.
10. Back up the Cisco Outbound Option private database using the SQL Server Enterprise Manager.

Note You must also upgrade the Cisco Outbound Option Dialers and their associated PGs for proper Outbound Option operation. See related upgrade information in Upgrade Cisco Outbound Option Dialer.

11. Use the data migration tool (EDMT) to update the Logger database.
12. Using the Domain Manager, add the Logger and Router instance to the appropriate Active Directory Instance Organizational Unit.
13. Run ICM *setup.exe* from the ICM Software CD on the Rogger. When the main setup screen appears, click Upgrade All.
14. Reboot the Rogger.
15. Run the Domain Conversion tool to migrate users to the new environment.
16. Install the latest Service Release and any required Engineering Specials on the Rogger.
17. Re-import the customer contact lists and do-not-call lists to the Outbound Option private database.
18. Install Cisco Security Agent with ICM Policy on the Rogger.

Upgrade Side B Central Controller Components

After completing the upgrade of Side A Central Controller, you have to perform the following procedures to bring the Side A Central Controller into service, before you can upgrade Side B:

1. Ensure network connectivity exists between the upgraded Cisco Unified ICM central controller components (Side A) (but not to other ICM nodes in the production network) by disabling Site1 (Side A) WAN and private router connections.
2. Using ICM Service Control, manually start the ICM services on the Side A router and Logger and the upgraded AW/HDS.
3. Ensure that operations are normal on the following components of the Side A Rogger by verifying:

   Basic operations:

   - Setup logs do not indicate errors or failure conditions.
   - All applicable components can “ping” public and private IP addresses.
   - Active Directory domain is populated with all the required users.
   - The schema upgrade is successful for all databases with no loss of data or data integrity.
   - Registry changes are correct and match contents of the setup logs.
   - All component services start without errors.
   - All general activities such as accessing SQL Server, running third-party software like VNC or PCAnywhere are not stopped by Cisco Security Agent.

   Router Operations:

   - The *ccagent* process is in service and connected to any PG that is located in Site1 of the test bed.
   - The *rtsvr* process is connected to the Primary Administration Workstation.

   Logger Operations:

   - The *recovery* process can start up normally, even though is not required (since Side B is not accessible by Side A at this point during the upgrade process).
   - Users are in the correct domain.
   - Configuration information is passed to the Router.
   - Replication process begins when the HDS comes online.

   HDS Operations:

   - The *updateaw* process indicates that it is waiting for work (ready to begin operations).
   - Replication process begins with no errors.

   Security Operations:

   - Specified users are able to use the ICM Configuration Manager.
   - Specified users are able to log into WebView and can access all previously existing public and private reports

   Script Editor Operations:

   - Previous settings for users remain unchanged when the Script Editor application is opened.
   - Validate that all the scripts yield the same results as prior to the upgrade.
   - You can create new scripts and open, edit, and delete scripts as well.

ICMDBA Operations:

- Import/Export functionality is present.
- Database space allocation and percentage (%) used are correct.

Support Tools Operations:

- You can acquire logs, capture registry information, and schedule collection of logs.

4. Using ICM Service Control, set the ICM services to AUTOSTART on each of the upgraded ICM components.

Note Call processing is impacted until the next three steps are completed, and therefore, must be executed at an appropriate pre-planned time.

5. Using ICM Service Control, stop the ICM Services on the Side B Logger and Router and on all the AW/HDS.
6. Reestablish the network connectivity between Site1 and the rest of the system.
7. Verify production system operation is running normally with the upgraded Side A Router and Logger.
8. Upgrade the Side B Rogger using the same procedures as listed in Upgrade Side A Central Controller Components (omit steps 10 and 17).
9. Using ICM Service Control, set the ICM services to AUTOSTART on the upgraded Side B Call Router and Logger.
10. Using ICM Service Control, start the ICM services on the new Side B Router and Logger.
11. Verify overall system operation.
12. Once data synchronization is complete between the Loggers, if possible, cycle the ICM services on the Side A Router and Logger.
13. Verify that the Side B takes over operations and that the system continues to operate normally.
14. Enable configuration changes by setting the *HKEY_LOCAL_MACHINE\ Software\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\ CurrentVersion\Configuration\Global\DBMaintenance* key to "0" on both Side A and Side B routers of the system being upgraded.

Note When enabling configuration settings on the Side B router, substitute 'RouterA' with 'RouterB' in the preceding registry key information.

15. Verify that you can now once again make configuration changes.
16. Upgrade all other Distributor AWs and/or HDS using the steps listed in Upgrade Distributor Administrator Workstation/Historical Database Server.

Upgrade Client Administrator Workstation

1. Using ICM Service Control, stop all ICM services on the AW.
2. Using ICM Service Control, change all ICM services on the AW to Manual Restart.
3. Perform a full system backup of the AW server so that it can be restored should a critical failure occur during the common ground upgrade process.

4. Uninstall the Cisco Security Agent and the ICM Policy.
5. Upgrade third-party software such as virus protection software and VNC or PC Anywhere.
6. Reboot the AW.
7. Install the ICM Support Tools Agent. It is not necessary to uninstall older versions of the Support Tools Agent.
8. Using the Domain Manager, add the AW instance to the appropriate Active Directory Instance Organizational Unit.
9. Run ICM *setup.exe* from the ICM Software CD. When the main setup screen appears, click Upgrade All to upgrade all ICM components on the AW.
10. Reboot the AW.
11. Install the latest Services Release and any required Engineering Specials on the AW.
12. Install Cisco Security Agent with ICM Policy on the AW.

Upgrade Peripheral Gateway (Side A and Side B)

While different Peripheral Gateways (PGs) can be upgraded at different times, you must upgrade Side A and Side B of the redundant PG pairs within the same maintenance window, along with the associated CTI Servers, CTI OS servers, and Cisco Outbound Option Dialers.

For proper Outbound Option operation, you must upgrade all Cisco Outbound Option Dialers during the same maintenance window as the Campaign Manager.

1. Using ICM Service Control, stop all ICM and CTI OS services on the Side A PG.
2. Using ICM Service Control, change all ICM and CTI OS services on the Side A PG to Manual Restart.
3. Perform a full system backup of the Side A PG server so that it can be restored in case a critical failure occurs.
4. Uninstall the Cisco Security Agent and the ICM Policy.
5. Upgrade third-party software such as virus protection software and VNC or PC Anywhere.
6. Reboot the Side A PG.
7. Install the ICM Support Tools Agent. It is not necessary to uninstall older versions of the Support Tools Agent.
8. Using the Domain Manager, add the PG instance to the appropriate Active Directory Instance Organizational Unit.
9. Run ICM *setup.exe* from the ICM Software CD. When the main setup screen appears, click Upgrade All to upgrade all ICM components on the Side A PG.
10. Run *setup.exe* from the CTI OS installation CD to install the latest version of CTI OS on Side A. It is not necessary to uninstall previous versions of CTI OS.
11. If this is a Cisco CallManager PG, upload the JTAPI Client from the Cisco CallManager using the information documented in Chapter 6 of the *IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition*. See Related Documentation for the URL.
12. Reboot the PG.
13. Install the latest Services Release and any required Engineering Specials on the Side A PG.
14. Install Cisco Security Agent with ICM Policy on the Side A PG.

15. If there are Cisco Outbound Option Dialers associated with the PG pair being upgraded which are on separate servers, upgrade all the Cisco Outbound Option Dialers now. For more information on upgrading Cisco Outbound Option Dialers, see Upgrade Cisco Outbound Option Dialer.

Note Call processing for the Peripheral being upgraded is affected until the next four steps are completed.

16. Using ICM Service Control, stop the ICM and CTI OS services on the Side B PG.
17. Using ICM Service Control, start all ICM and CTI OS services on the Side A PG.
18. Using ICM Service Control, set all of the ICM and CTI OS processes on the Side A PG to AUTOSTART.
19. Verify the proper operation of the peripheral running on the upgraded Side A PG (call flows, CTI desktops and other applications, and Cisco Outbound Option Dialers).
20. Repeat the above procedures to upgrade the Side B PG.
21. Using ICM Service Control, start all ICM and CTI OS services on the Side B PG.
22. Using ICM Service Control, set all of the ICM and CTI OS processes on the upgraded Side B PG to AUTOSTART.
23. Verify that the ICM components on the Side B PG start up and come into service by reviewing the process windows and/or log files.
24. Using ICM Service Control, stop all ICM and CTI OS services on the Side A PG.
25. Verify that the upgraded Side B PG becomes active and the peripheral running on the upgraded Side B PG (call flows, CTI desktops and other applications, and Cisco Outbound Option Dialers) is properly operating.
26. Using ICM Service Control, restart the ICM and CTI OS services on the Side A PG.

Upgrade Cisco Outbound Option Dialer

1. Using ICM Service Control, stop all ICM services on the Cisco Outbound Option Dialer.
2. Using ICM Service Control, change all ICM services on the Cisco Outbound Option Dialer to Manual Restart.
3. Perform a full system backup of the Cisco Outbound Option Dialer server so that it can be restored in case a critical failure occurs.
4. Uninstall the Cisco Security Agent and the ICM Policy.
5. Upgrade third- party software such as virus protection software and VNC or PC Anywhere.
6. Reboot the Cisco Outbound Option Dialer.
7. Install the ICM Support Tools Agent. It is not necessary to uninstall older versions of the Support Tools agent.
8. Using the Domain Manager, add the Cisco Outbound Option Dialer instance to the appropriate Active Directory Instance Organizational Unit.
9. Run ICM *setup.exe* from the ICM Software CD. When the main setup screen appears, click Upgrade All to upgrade all ICM components on the Cisco Outbound Option Dialer.
10. Reboot the Cisco Outbound Option Dialer.
11. Install the latest Services Release and any required Engineering Specials on the Cisco Outbound Option Dialer.

12. Install Cisco Security Agent with ICM Policy on the Cisco Outbound Option Dialer.

Upgrade CTI OS Agent and Supervisor Desktop

1. Stop the CTI OS Agent or Supervisor Desktop application that is running on the machine.
2. Run the CTI OS Client install from the ICM Software CD, updating configuration data as prompted.
3. Reboot the machine if you are directed to do so.

Upgrade from Windows 2000 to Windows Server 2003

Upgrading from Windows 2000 to Windows Server 2003 requires a considerable amount of planning and preparation.

Listed below are the main points to be aware of prior to performing the upgrade:

- Check the source Operating System revision and its edition. Determine the nearest equivalent target edition before implementing the upgrade process.
- Be aware that you can only upgrade to an equivalent or a higher Operating System. It is not possible to ‘downgrade” to a lower Operating System, since you may lose some functionality in the process.
- Ensure that the computer being upgraded meets the recommended system requirements.
- Make sure that all hardware components and third-party software are compatible with the Operating System. The hardware requirements for the Windows Server 2003 Operating System are exceeded by the ICM hardware requirements specified in the BOMs.

Note 5.0 BOM compliance is the minimum requirement for ICM 7.0. The recommended hardware for ICM 7.0 is the 7.0 BOM.

For a comprehensive list of hardware and software supported by the Windows Server 2003 Operating System, see the *Windows Server Catalog* at the Microsoft website.

For more information on upgrading to Windows 2003, see the *Windows Server 2003 Upgrade Assistance Center* information at the Windows Server 2003 Support website or the web-based product documentation at the *Product Documentation for Windows Server 2003* website.

After upgrading the ICM system on Windows 2000 as listed above, upgrade the Operating System to Windows Server 2003 and apply the automated hardening provided by the ICM system.

Do this by either:

- Rerunning ICM Setup and choosing to apply the hardening when prompted.
- Applying the security hardening from the command line. See Chapter 4 of the *Security Best Practices Guide for ICM and IPCC Enterprise & Hosted Editions* at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/coreicm7/config7/icme70sg.pdf

Upgrading the OS on a WebView Server

When upgrading the Operating System on a server with the WebView Server software installed, do the following:

1. Uninstall all ICM Engineering Specials and Service Releases.
2. Upgrade the Operating System to Windows 2003 with the latest supported Service Pack.

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

Note Do not reinstall the JDK or the EAServer.

4. Run ICM *setup.exe* from the ICM Software CD on the WebView server.
5. Edit the WebView component and continue through the setup process for the WebView component to reinstall and reconfigure the WebView files.
6. Reinstall all the ICM Service Releases and Engineering Specials.

Upgrade Cisco CallManager Clusters

Follow the best practices specified in the *Developing Migration Strategies for Cisco CallManager 5.0* for migrating and upgrading the Cisco CallManager cluster.

Be aware of the following before you start the Cisco CallManager upgrade process:

- Ensure that a working SFTP server is available to provide network location for backup after the upgrade.
- It is highly recommend that a working NTP server is available to provide network time for all cluster machines.
- If CDR records are not required to be migrated, purge the CDR records to minimize the impact on time before running the DMA.
- It is not possible to migrate the Customer Background images, Custom TFTP files, Custom Music On Hold files, Customer Ring Tones. You need to backup these files and reload them after the upgrade is complete.
- Upgrade from Windows will fail unless both the forward and reverse DNS entries are set up for the subscriber.

Upgrade only those Cisco CallManager clusters in the test bed that are targeted for upgrade as follows:

1. Back up the existing Cisco CallManager 4.1(3)SR1 system on BARS.

Note If possible, we highly recommend that you preserve a copy of the hard drive(s).

2. Run the latest Upgrade Assistant tool and verify that the cluster is ready for the upgrade. Correct any errors that are encountered before proceeding to the next step.
3. Download and install the Data Migration Assistant (DMA) tool and run a DMA backup from the publisher.

   System data and configuration information are gathered and stored on a network storage location that you specify. The exported data is verified by the Upgrade Assistant.
4. If you encounter any errors during the migration process, correct the errors or contact TAC for further assistance. Re-run the DMA as needed.
5. Write down the following information before you start the upgrade:
   - List of services running on each node to verify that they are operational after the upgrade
   - Number of registered devices such as gateways, phones, and media resources
   - Number of devices configured in the database such as trunks, users, and CTI route points
   - List of phones that are encrypted

Note Make sure that the migration of data is completed successfully before you start the upgrade procedure. Also ensure that the DVD ROM drive is operational by testing it.

6. Using the Cisco Unified CallManager 5.0 Install DVD, perform the upgrade of the publisher first and then of all the subscribers in the cluster.

Upgrading the Publisher

When upgrading the publisher, remember to do the following:

- Select "Windows Upgrade" as the Type of Installation.
- Specify that this is the first node in the cluster.
- Configure subnets appropriately to ensure that all the nodes in the cluster will synchronize with the correct publisher.
- Download the License Manager file and upload the required licenses for the cluster.

Note One license file is needed per Unified CallManager cluster. You will require the MAC address of the publisher to generate the license. Once generated, these files can be reused as long as the publisher's MAC address remains unchanged.

Upgrading the Subscriber

When upgrading the subscribers, remember to do the following:

- Make sure that the newly upgraded publisher is available.
- Select "Basic Install" as the Type of Installation.
- Specify that this NOT the first node in the cluster.
- Upgrade no more than four subscribers simultaneously.

Reinstalling Latest JTAPI Client

1. On the Unified CallManager PGs, upload the JTAPI Client from the Unified CallManager using the information documented in Chapter 6 of the *IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition*. See Related Documentation for the URL.
2. Reboot the PG.

Recovering from a Failed Upgrade

In case the upgrade to Unified CallManager 5.0(2) fails, you have one of following two options to go back to your Cisco CallManager Release 4.1(3)SR1 setup:

- If you have preserved your hard drive(s), you can swap the hard drive(s) out.
- If not, you have to reinstall Cisco CallManager Release 4.(3)SR1 software and reload the old system data from the backup you created in step 1.

Upgrade Gateways and Gatekeepers

1. Copy the correct image on each switch via TFTP.
2. Modify the boot system configuration to enable loading of the new image.
3. Reboot the switch. The switch reads the modified configuration and reloads with the new image.

Related Documentation

Compatibility Documentation

- *Cisco CallManager Compatibility Matrix*: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm
- *IPCC Enterprise Software Compatibility Guide*: http://www.cisco.com/application/pdf/en/us/guest/products/ps1844/c1609/ccmigration_09186a008031a0a7.pdf
- *Cisco Response Solutions (CRS) Software and Hardware Compatibility Guide*: http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/crscomtx.pdf

Cisco CallManager Installation and Upgrade Documentation

- *Known Upgrade Issues in Release Notes for Cisco Unified CallManager Release 5.0(2)*: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_note09186a008062bd3b.html
- *Installing Cisco Unified CallManager Release 5.0(2)*: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guide09186a0080631ef5.html
- *Upgrading Cisco Unified CallManager Release 5.0(2)*: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guide09186a0080631df2.html
- *Disaster Recovery System Administration Guide Release 5.0(2)*: http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide09186a0080631a03.html
- *Data Migration Assistant User Guide Release 5.0(2)*: http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide09186a0080631d80.html
- *Installing Cisco CallManager Release 4.1(3)*: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guide09186a00803f5c57.html
- *Upgrading Cisco CallManager Release 4.1(3)*: http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_installation_guide_book09186a00803bea43.html
- *Using Cisco CallManager Upgrade Assistant Utility 4.1(3)*: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guide09186a00803f5c59.html

Contact Center Installation and Upgrade Documentation

- *Known Upgrade Issues in Release Notes:* http://www.cisco.com/application/pdf/en/us/guest/products/ps1001/c1178/ccmigration_09186a00805670e0.pdf
- *IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition*: http://www.cisco.com/application/pdf/en/us/guest/products/ps1844/c1097/ccmigration_09186a00804d73b7.pdf
- *Cisco IPCC Gateway Deployment Guide ICM/IPCC Enterprise Edition:* http://www.cisco.com/application/pdf/en/us/guest/products/ps1001/c1097/ccmigration_09186a0080626383.pdf
- *System IPCC Enterprise Installation and Configuration Guide*: http://www.cisco.com/application/pdf/en/us/guest/products/ps1844/c1676/ccmigration_09186a00804d8b1c.pdf
- *Pre-installation Planning Guide for Cisco ICM Enterprise Edition:* http://www.cisco.com/application/pdf/en/us/guest/products/ps1001/c1097/ccmigration_09186a00804d7115.pdf
- *ICM Installation Guide for Cisco ICM Enterprise Edition*: http://www.cisco.com/application/pdf/en/us/guest/products/ps1001/c1097/ccmigration_09186a00804d7106.pdf
- *Upgrade Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*: http://www.cisco.com/application/pdf/en/us/guest/products/ps1001/c1952/ccmigration_09186a00805e1ea2.pdf
- *Cisco ICM/IPCC 7.0 Upgrade Mitigation Strategies White Paper*: http://www.cisco.com/application/pdf/en/us/guest/products/ps1001/c1952/ccmigration_09186a0080520003.pdf
- *Cisco Customer Voice Portal (CVP) Installation Guide*: http://www.cisco.com/application/pdf/en/us/guest/products/ps1006/c1097/ccmigration_09186a0080552e0b.pdf
- *Cisco CVP VoiceXML 3.1 Installation Guide:* http://www.cisco.com/application/pdf/en/us/guest/products/ps1006/c1097/ccmigration_09186a0080552e11.pdf
- *Cisco CAD Installation Guide*: http://www.cisco.com/application/pdf/en/us/guest/products/ps427/c1097/ccmigration_09186a00805e2465.pdf
- *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions:* http://www.cisco.com/application/pdf/en/us/guest/products/ps14/c1676/ccmigration_09186a00804d2a89.pdf

Cisco Unity Connection Installation and Upgrade Documentation

- *Cisco Unity Connection Installation Guide*: http://www.cisco.com/en/US/products/ps6509/products_installation_guide_book09186a00805201e8.html

- *Cisco Unity Connection Reconfiguration and Upgrade Guide*: http://www.cisco.com/en/US/products/ps6509/products_upgrade_guides_book09186a0080511ad7.html

CRS and IP IVR Installation and Upgrade Documentation

- *Known Upgrade Issues in Release Notes*: http://www.cisco.com/application/pdf/en/us/guest/products/ps6879/c1178/ccmigration_09186a008063b195.pdf
- *Cisco CRS Installation Guide*: http://www.cisco.com/application/pdf/en/us/guest/products/ps6879/c1097/ccmigration_09186a0080610e12.pdf
- *Getting Started with Cisco IP IVR CRS*: http://www.cisco.com/application/pdf/en/us/guest/products/ps6879/c1689/ccmigration_09186a0080611818.pdf
- *Backup and Restore System for Cisco Customer Response Solutions 4.5*: http://www.cisco.com/application/pdf/en/us/guest/products/ps6879/c1097/ccmigration_09186a0080612a78.pdf