Installation and Configuration Guide for Cisco Unified Contact Center Domain Manager

Release 10.0.1

April 2014 (Updated 17 April 2014)

Corporate Headquarters
Cisco Systems, Inc.
170, West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Table of Contents

Table of Contents ..... **iii**
Preface ..... **xi**
Purpose xi
Audience xi
Organization xi
Related Documentation xii
Document Conventions xiii
Obtaining Documentation, Obtaining Support and Security Guidelines xiv
Documentation Feedback xiv
1 Planning Your Installation **1**
1.1 About Your Installation 1
1.2 Deployment Specifics 1
1.3 Infrastructure Software 1
1.4 Unified CCDM Components 2
1.5 Deployment Models 2
2 Installation Requirements **5**
2.1 Installation Prerequisites 5
2.1.1 About the Installation Prerequisites 5
2.1.2 General Requirements 5
2.1.3 Windows Requirements 5
2.1.4 Additional Software Requirements 5
2.1.4.1 Database Servers 6
2.1.4.2 App/Web Servers 6
2.1.5 Clients running the Web Application 6
2.2 Firewall Configuration 6
2.2.1 About Firewall Configuration 6
2.2.2 Web Server Port Usage 7
2.2.3 Unified CCDM Database Server Port Usage 7
2.2.4 Cisco Unified CCE Port Usage 8

2.2.5 Domain Controllers for Unified CCE Instances Port Usage 8
2.2.6 Cisco Unified CM Port Usage 8
2.2.7 Other Information 8
2.3 Security Considerations 9
2.3.1 Mandatory Security Configuration 9
2.3.2 Optional Security Configuration 9
3 Windows and SQL Installation and Configuration 11
3.1 Windows Configuration 11
3.1.1 Firewalls 11
3.1.2 All Unified CCDM Servers 11
3.2 SQL Server 11
3.2.1 Install SQL Server 11
3.2.2 Configure SQL Server Network Protocols 13
3.2.3 Configure Windows Firewall for SQL Server 14
3.2.4 SQL Server Backup Guidelines 14
3.3 User Accounts 14
3.3.1 Unified CCDM Service Accounts 14
3.4 Optional Security Configuration 15
3.4.1 Disable Anonymous Sessions 15
3.4.2 Disable Cached Logins 16
3.4.3 Disable DCOM 16
3.4.4 Enable Mandatory SMB Signing for all Unified CCDM Servers 17
3.4.5 Disable SSL V2 17
3.4.6 Disable Remote Access to Unified CCDM Servers 18
4 Unified CCDM Installation 19
4.1 Before You Start 19
4.1.1 Installing Dual-Sided Systems 19
4.1.2 Recording Your Settings 19
4.2 The Unified CCDM Installer 20
4.2.1 About the Unified CCDM Installer 20
4.2.1.1 Starting the Installer 20

4.2.1.2 Installation Prerequisites 20
4.2.2 Install the Database Installer 20
4.2.3 Install the Portal Database 22
4.2.4 Install the App/Web Server 26
4.2.5 Install the Second Side (Replicated Systems Only) 28
4.3 Support Tools 28
4.3.1 About the Support Tools 28
4.3.2 Install the Diagnostic Framework 28
5 Unified CCDM Configuration 30
5.1 About Unified CCDM Configuration 30
5.2 Configure Unified CCE Admin Workstations 30
5.3 Configure Unified CCE Provisioning 31
5.3.1 About Provisioning Configuration 31
5.3.2 Set Up ConAPI 32
5.3.3 Set Up the CMS Server 32
5.4 Configure the Unified CCDM Cluster 34
5.4.1 About Cluster Configuration 34
5.4.2 Start ICE Cluster Configuration 34
5.4.3 Set Up Unified CCDM Servers 34
5.4.4 Configure Cisco Unified CCE Servers 37
5.4.4.1 Unified CCE Deployment Models 37
5.4.4.2 Unified CCDM Connection Requirements 37
5.4.4.3 Configuring the Servers 38
5.4.5 Configure Cisco Unified CM Servers 41
5.4.6 Configure Cisco Unified CVP Servers Wizard 43
5.4.7 Configure Avaya CMS Servers Wizard 45
5.4.8 Create and Map Tenants 46
5.4.8.1 About Creating and Mapping Tenants 46
5.4.8.2 Creating Tenants and Folders 47
5.4.8.3 Creating an Equipment Mapping 47
5.5 Replication 48

5.5.1 About Replication 48
5.5.1.1 About the Replication Manager 48
5.5.1.2 About The Snapshot Process 48
5.5.1.3 About Replication Publications 49
5.5.2 Configure Replication 49
5.5.3 Monitor the Replication Snapshot 51
5.6 Unified CVP Media File Upload 53
5.6.1 About Unified CVP Media File Upload 53
5.6.2 Prepare the Configuration 53
5.6.3 Configure Unified CVP Media File Upload - Windows Server 2003 53
5.6.3.1 Configure DFS for Unified CVP Media File Upload 54
5.6.3.2 Configure DFS Root Targets 54
5.6.3.3 Configure File Replication for Unified CVP Media File Upload 55
5.6.4 Configure Unified CVP Media File Upload - Windows Server 2008 55
5.6.4.1 Create a Shared Namespace 55
5.6.4.2 Configure Replication 56
5.6.4.3 Share and Publish the Replicated Folder 57
5.6.4.4 Configure the Replicated Folder for Media File Upload 58
5.6.5 Test the CVP Upload Configuration 58
6 Post-Installation Steps 59
6.1 About Post-Installation Steps 59
6.2 Configure SSL for Unified CCDM and Web Services 59
6.2.1 About Configuring SSL for Unified CCDM and Web Services 59
6.2.2 Obtain a Digital Certificate 60
6.2.3 Configure SSL for Unified CCDM 61
6.2.4 Grant Network Service Rights to the Certificate 62
6.2.5 Obtain the Certificate Thumbprint 62
6.2.6 Configure Web Services to use the Certificate 63
6.2.7 Test the Certificate Installation 64
6.3 Configure Single Sign-On 64
6.3.1 About Single Sign-On 64

6.3.2 Set Up Administrator Account 65
6.3.3 Configure SSO Authentication 65
6.3.4 Manage Users with Single Sign-On 66
6.4 Configure Antivirus Options 67
6.5 Performance Tuning Checklists 67
6.5.1 Web Server 68
6.5.2 Database Server 68
6.6 Final Post-Installation Actions 68
6.6.1 Restart the System 68
6.6.2 Log in to Unified CCDM 68
6.6.3 Verify the Installation 69
7 Upgrading From a Previous Version 70
7.1 About the Upgrade Procedure 70
7.2 About Upgrading Dual-Sided Systems 70
7.3 Validating an Upgrade 71
8 Single-Sided Upgrade 73
8.1 About a Single-Sided Upgrade 73
8.2 Checklist for Single-Sided Upgrades 73
8.3 Prepare the Unified CCDM Servers 74
8.3.1 Stop the Unified CCDM Services 74
8.3.2 Back up the Unified CCDM Portal Database 75
8.4 Uninstall Existing Unified CCDM Software 75
8.4.1 Uninstall the Database Server Components 75
8.4.2 Uninstall the App/Web Server Components 76
8.5 Install New Unified CCDM Components and Upgrade Portal Database 76
8.5.1 Install the Database Installer 76
8.5.2 Upgrade the Portal Database 77
8.5.3 Install the App/Web Server 78
8.5.4 Configure the Unified CCE Config Web Service 80
8.6 Restart and Validate 82
8.6.1 Restart the Unified CCDM Services 82

8.6.2 Validate the Upgrade 83
9 Total Outage Upgrade 84
9.1 About a Total Outage Upgrade 84
9.2 Checklist for Total Outage Upgrades 84
9.3 Prepare Unified CCDM Servers 85
9.3.1 Stop the Unified CCDM Services 85
9.3.2 Remove Portal Database Replication 86
9.3.3 Back up the Portal Databases 87
9.4 Uninstall Existing Unified CCDM Software 87
9.4.1 Uninstall the Database Server Components 87
9.4.2 Uninstall the App/Web Server Components 88
9.5 Install New Components and Upgrade Portal Database 88
9.5.1 Install the Database Installer 88
9.5.2 Upgrade the Portal Database 90
9.5.3 Install the App/Web Server 91
9.5.4 Configure the Unified CCE Config Web Service 92
9.6 Restore Replication 95
9.6.1 Restore Unified CCDM Database Replication 95
9.6.2 Monitor the Replication Snapshot 97
9.7 Restart and Validate 98
9.7.1 Restart the Unified CCDM Services 98
9.7.2 Validate the Upgrade 99
10 Split Side Upgrade 100
10.1 About a Split Sided Upgrade 100
10.2 Checklist for Split Side Upgrades Part 1 100
10.3 Prepare the Unified CCDM Servers (Side A) 101
10.3.1 Stop the Unified CCDM Services (Side A) 101
10.3.2 Remove Portal Database Replication 103
10.3.3 Back up the Portal Databases (Side A) 103
10.4 Uninstall Existing Unified CCDM Software on Side A 104
10.4.1 Uninstall the Database Server Components (Side A) 104

10.4.2 Uninstall the App/Web Server Components (Side A) 104
10.5 Install New Unified CCDM Components and Upgrade Database (Side A) 104
10.5.1 Install the Database Installer (Side A) 104
10.5.2 Upgrade the Portal Database (Side A) 106
10.5.3 Install the App/Web Server (Side A) 107
10.6 Finalize Configuration (Side A) 109
10.6.1 Force Failover Connections to the Active Side 109
10.6.2 Update Side B to Enable Provisioning and Import (Optional) 110
10.6.3 Update Provisioning on the Unified CCE AW 110
10.6.4 Update Provisioning on the Side B Database Server 111
10.6.5 Configure the Unified CCE Config Web Service 112
10.7 Restart (Side A) 114
10.7.1 Restart the Unified CCDM Services 114
10.8 Checklist for Split Side Upgrades Part 2 114
10.9 Prepare the Unified CCDM Servers (Side B) 115
10.9.1 Stop the Unified CCDM Services (Side B) 115
10.9.2 Back up the Portal Database (Side B) 116
10.10 Uninstall Existing Unified CCDM Software(Side B) 117
10.10.1 Uninstall the Database Server Components (Side B) 117
10.10.2 Uninstall the App/Web Server Components (Side B) 117
10.11 Install New Unified CCDM Components and Upgrade Database (Side B) 118
10.11.1 Install the Database Installer (Side B) 118
10.11.2 About Upgrading the Side B Database 119
10.11.3 Upgrade Side B Database (Option 1) 120
10.11.4 Restore Side B Database from the Side A Backup (Option 2) 121
10.11.5 Install the Unified CCDM App/Web Server (Side B) 121
10.12 Finalize Configuration (Side B) 123
10.12.1 Stop Forcing Failover Connections to the Active Side 123
10.12.2 Restore Unified CCDM Database Replication 123
10.12.3 Monitor the Replication Snapshot 125
10.13 Restart and Validate (Side B) 127

10.13.1 Restart the Unified CCDM Services 127
10.13.2 Validate the Upgrade 127
11 Uninstalling Unified CCDM 128
11.1 About Uninstalling Unified CCDM 128
11.2 Remove Database Replication 128
11.3 Uninstall the Database Components 129
11.4 Remove the Database Catalog 129
11.5 Uninstall the Other Components 130
12 Troubleshooting 131
12.1 About Installer Logs 131

Preface

Purpose

This document explains how to install the Unified Contact Center Domain Manager (Unified CCDM) components.

Audience

This document is intended for System Administrators with knowledge of their Unified Contact Center Enterprise (Unified CCE) system architecture. Microsoft SQL Server database administration experience is also helpful.

Organization

The sections of this guide are as follows:

Chapter 1	Planning Your Installation	Introduces Unified CCDM, including its integration with Unified CCE.
Chapter 2	Installation Requirements	Lists the prerequisites for Unified CCDM installation and provides recommendations for pre installation platform configuration.
Chapter 3	Windows and SQL Installation and Configuration	Describes how to setup the Microsoft SQL Server.
Chapter 4	Unified CCDM Installation	Provides instructions for the installation of all Unified CCDM components.
Chapter 5	Unified CCDM Configuration	Describes post-installation configuration of Unified CCDM, including setting up replication and uploading .wav files for voice announcements. The procedure for configuring a Unified CCDM server cluster is detailed as well as how to use the Unified CCDM Replication Manager to replicate data between Database Servers. Web and Database component server performance checklists are also provided.
Chapter 6	Post-Installation Steps	Describes the post-installation options and the system checks for the Unified CCDM platform.
Chapter 7	Upgrading From a Previous Version	Explains the various options for upgrading an existing installation of Unified CCDM without losing your data.

Chapter 8	Single-Sided Upgrade	Describes how to upgrade a single-sided deployment.
Chapter 9	Total Outage Upgrade	Describes how to upgrade a dual-sided deployment in one operation.
Chapter 10	Split Side Upgrade	Describes how to upgrade a dual-sided deployment in two stages, one side at a time.
Chapter 11	Uninstalling Unified CCDM	Describes how to remove Unified CCDM from your servers.
Chapter 12	Troubleshooting	Describes how to enable logging for the Unified CCDM Installer and how to apply database permissions after the Installer has completed.

Related Documentation

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

- Related documentation includes the documentation sets for Cisco CTI Object Server (CTIOS), Cisco Agent Desktop (CAD), Cisco Agent Desktop - Browser Edition (CAD-BE), Cisco Unified Customer Voice Portal (CVP),Cisco Unified IP IVR, Cisco Unified Intelligence Center, and Cisco Support Tools.
- For documentation for these Cisco Unified Contact Center products, go to http://www.cisco.com/cisco/web/psa/default.html, click **Voice and Unified Communications**, then click **Customer Contact**, then click **Cisco Unified Contact Center Products** or **Cisco Unified Voice Self-Service Products**, then click the product/option you are interested in.
- For troubleshooting tips for these Cisco Unified Contact Center products, go to http://docwiki.cisco.com/wiki/Category:Troubleshooting, then click the product/option you are interested in.
- Documentation for Cisco Unified Communications Manager is accessible from: http://www.cisco.com/cisco/web/psa/default.html.
- Technical Support documentation and tools are accessible from: http://www.cisco.com/en/US/support/index.html.
- The Product Alert tool is accessible from (sign in required): http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice.

- For information on the Cisco software support methodology, refer to *Software Release and Support Methodology: ICM/IPCC* available at (sign in required): http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/prod_bulletins_list.html.

For a detailed list of language localizations, refer to the *Cisco Unified ICM/Contact Center Product and System Localization Matrix* available at the bottom of the following page: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html.

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as entries, keys, buttons, folders and submenu names. For example: • Choose **Edit > Find** • Click **Finish**
italic font	Italic font is used to indicate the following: • To introduce a new term; for example: A *skill group* is a collection of agents who share similar skills • For emphasis; for example: *Do not* use the numerical naming convention • A syntax value that the user must replace; for example: IF (*condition, true-value, false-value*) • A title of a publication; for example: Refer to the *Cisco CRS Installation Guide*
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays; for example: `<html><title>Cisco Systems, Inc. </title></html>`
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output • A character string that the user enters but that does not appear on the window, such as a password

Obtaining Documentation, Obtaining Support and Security Guidelines

For information on obtaining documentation, obtaining support, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

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

Documentation Feedback

You can provide comments about this document by sending an email message to the following address: ccbu_docfeedback@cisco.com

We appreciate your comments.

1 Planning Your Installation

1.1 About Your Installation

A successful installation of Unified CCDM requires some understanding of the platform components, the environment in which they are deployed and how they are configured in a cluster of linked servers. File systems and storage options are also discussed as well as user accounts and security considerations in an internet facing environment.

1.2 Deployment Specifics

Unified CCDM Resource Management deployments are limited to standard and hosted Unified CCE deployments, with the following restrictions:

Each configured Unified CCE instance must have its own:

- Unified ICM instance.
- Dedicated Admin Workstation Real Time Distributor Server. Multiple Distributor instances on a single server are not allowed.
- Dedicated Admin Workstation CMS Server. Multiple CMS Server instances on a single server are not allowed.

Unified CCDM is only supported on Unified CCE 7.1 and later.

1.3 Infrastructure Software

Unified CCDM requires:

- Windows 2008 Server R2 with Service Pack 1
- SQL Server 2008 R2 Standard Edition with Service Pack 2.

1.4 Unified CCDM Components

A Unified CCDM installation comprises the following components.

- the **Database Server**, which holds information about resources (such as agents, skill groups and dialed numbers) and actions (such as phone calls and agent state changes) in the system. It consists of:
  - the **Portal Database** , which holds the data that has been provisioned through Unified CCDM or imported from Unified CCE
  - the **Data Import Server**, which imports and synchronizes resources and changes to resources from back-end contact center systems (for example, Unified CCE)
  - the **Provisioning Server**, which applies resource changes made by Unified CCDM users to the back-end contact center systems
  - the **Partitioning Server**, which manages the creation and removal of Unified CCDM partition tables, used to store contact center data
- the **App/Web Server** which provides two components for interfacing with Unified CCDM:
  - **Application Server** delivers application services such as search, security and resilience to the Unified CCDM Web Server
  - **Web Server** provides the web front end that allows users perform resource management and administrative tasks.

1.5 Deployment Models

In many environments, Unified CCDM is installed using a dual-sided deployment model to provide load balancing, resiliency, and high availability. For deployments that require layered security, such as Internet-facing environments, both sides are split across separate Database Servers and App/Web Servers are separated by a demilitarized zone (DMZ).

Because Unified CCDM scales up with equipment and scales out with servers, a variety of cost-effective deployment models are possible. Review the Hardware and System Software Specification (Bill of Materials) for Cisco Unified ICM / Contact Center Enterprise & Hosted carefully prior to deployment model selection.

Each of the following deployment models assumes the possibility of a dual-sided server configuration that replicates data between sites.

- **Single Tier (Dedicated Server)**. All Unified CCDM components are installed on a single dedicated server.
- **Two Tier (Secure Deployment)**. Unified CCDM Application and Web components are hosted on one server. The Provisioning, Data Import and Database components are hosted on a second server.

Figure 1.1 "Component Layout for a Single Tier Deployment" describes the software installation layout for a single tier deployment. All components reside on a single server. This configuration can optionally have a second side in the same configuration for resilience.

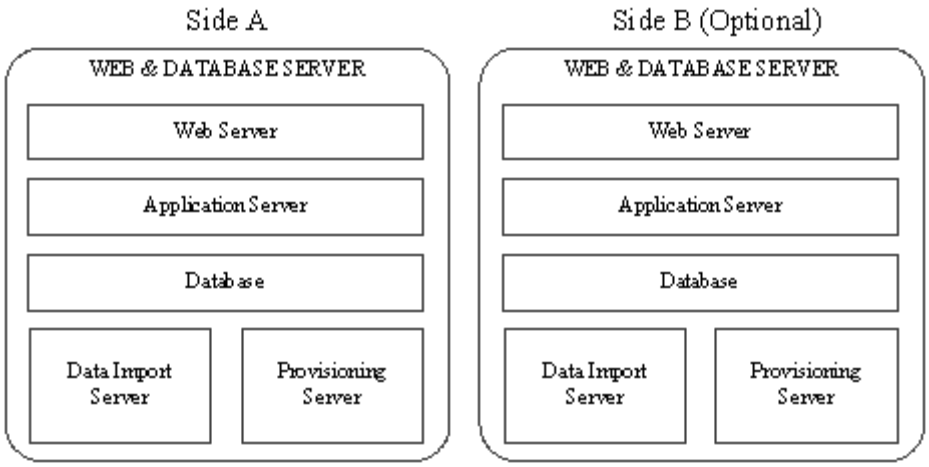

Figure 1.1 Component Layout for a Single Tier Deployment

Figure 1.2 "Component Layout for a Dual Tier Deployment" below, describes the software installation layout for a dual tier deployment. The web server and application server components reside on a separate server. This configuration can optionally have a second side in the same configuration for resilience.

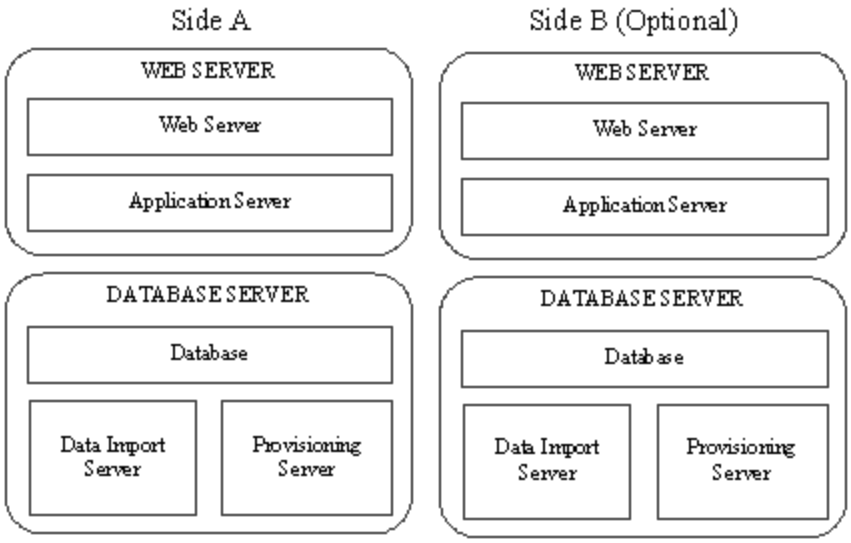

Figure 1.2 Component Layout for a Dual Tier Deployment

2 Installation Requirements

2.1 Installation Prerequisites

2.1.1 About the Installation Prerequisites

This section describes the installation prerequisite requirements for Unified CCDM.

The Unified CCDM Installer checks that the prerequisites for each component are present and correctly configured before allowing you to install that component. Where possible, prerequisite software is included with the Unified CCDM Installer, and is installed and configured directly from the Installer. SQL Server is licensed separately, so is not included with the Unified CCDM Installer.

2.1.2 General Requirements

This section describes the general requirements for your installation.

- Do not install any Unified CCDM component on a domain controller.
- Unified CCDM server names must consist of alphanumeric characters only, without underscores or hyphens.
- Unified CCDM can run on systems equipped with IPv6 hardware, but all Unified CCDM Servers must have an IPv4 address and IPv6 must be disabled on the NIC used by Unified CCDM.
- Unified CCDM does not support SQL Server named instances. All SQL Server installations must use the default instance name.
- It is recommended that the SQL Server Temp DB directory and Temp DB log directory are *not* located on the same disk as the operating system.

2.1.3 Windows Requirements

Ensure these requirements are satisfied before starting the installation.

All Unified CCDM servers require the following version of Windows:

- Windows Server 2008 R2 SP1.

2.1.4 Additional Software Requirements

This section lists the additional software required for each Unified CCDM server. Detailed instructions for installing and configuring these items are provided at the appropriate point in the installation instructions.

2.1.4.1 Database Servers

The following software is required on all Unified CCDM Database Servers:

- Microsoft SQL Server 2008 R2 64 bit Standard Edition
- Microsoft SQL Server 2008 R2 Workstation Components
- Microsoft SQL Server 2008 R2 Service Pack 2 (64 bit).

2.1.4.2 App/Web Servers

There are no additional software requirements for the App/Web Servers.

2.1.5 Clients running the Web Application

The Unified CCDM web application supports the following browsers:

- Internet Explorer version 7 or later
- Google Chrome version 25 or later
- Mozilla Firefox version 18 or later.

2.2 Firewall Configuration

2.2.1 About Firewall Configuration

Firewalls may be deployed between the various Unified CCDM servers (to create a DMZ) and possibly also between the Unified CCDM database servers and the Unified CCE AWs. In such configurations, the appropriate firewall ports must be opened to both-way traffic.

The Windows 2008 R2 platform incorporates its own software based firewall that must be configured to allow the various components of Unified CCDM to communicate with one another in a distributed environment. When configuring the Windows firewall it is recommended that port restrictions are limited to only the servers that require the specified communications channels.

The incoming firewall requirements for the Unified CCDM software components are listed in the tables below.

These tables do not include standard Windows ports such as DNS and Kerberos, or the ports required to access the Unified CCDM servers for support purposes (either Terminal Services or Remote Desktop).

Note
If required, configure the firewall ports before you install Unified CCDM.

2.2.2 Web Server Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Used by	Usage
HTTP	TCP	80	End User	Web application
HTTPS	TCP	443	End User	Web application
Web Service Subscriptions	TCP	8083	Customer Applications	Customer-specific
Web Service Resource Management	TCP	8085	Customer Applications	Customer-specific
Web Service Analytic Data	TCP	8087	Customer Application and ISE integration	Customer-specific and ISE integration

2.2.3 Unified CCDM Database Server Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Servers Requiring Access	Usage
SQL Server	TCP	1433	Database Servers, Application Servers	General
DTC	TCP	2103	Database Servers	Audit Archive
DTC	TCP	2105	Database Servers	Audit Archive
DTC (RPC)	TCP	135	Database Servers	Audit Archive
DTC (RPC)	TCP	5000-5100**	Database Servers	Audit Archive
NetBIOS File Share	UDP	137-138	Database Servers and Application Servers	Replication, Unified CVP File Upload
NetBIOS File Share	TCP	139	Database Servers and Application Servers	Replication, Unified CVP File Upload
SMB (DFS)	TCP	445	Database Servers and Application Servers	Unified CVP File Upload File***
ConAPI Local Registry	TCP	2099*	Unified CCE Admin Workstation	Provisioning
ConAPI Local Port	TCP	3333*	Unified CCE Admin Workstation	Provisioning

* Default value for Side A - use configured in Cluster Configuration.

** Dynamically assigned RPC port range used by MSDTC. Configured in registry: HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\InternetAfter each change the machine must be restarted.

*** Only required if Unified CVP Media File Upload is configured. If configured, also ensure that required ports for the Distributed File Systems are open on the Domain Controller.

2.2.4 Cisco Unified CCE Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Servers Requiring Access	Usage
SQL Server	TCP	1433	Database Servers and Application Servers	Importing Dimension Data, Provisioning Activities.
ConAPI Remote Registry	TCP	2099*	Database Servers	Provisioning
CMS Node	UDP	9000	Database Servers	Ping Port for ConAPI services
Web Service API	TCP	443	Database Servers	Provisioning

* Default value for Side A - use configured in Cluster Configuration.

2.2.5 Domain Controllers for Unified CCE Instances Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Servers Requiring Access	Usage
LDAP	TCP	389	Database Servers and Application Servers	Supervisor domain account provisioning

2.2.6 Cisco Unified CM Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Servers Requiring Access	Usage
AXL Web Service (HTTPS)	TCP	443	Database Servers	Importing and Provisioning

2.2.7 Other Information

When configuring DTC and File Sharing on the Windows 2008 R2 firewall then the appropriate options within the Windows 2008 R2 Firewall Exceptions list may be selected. These options are labeled as follows:

- Distributed Transaction Coordinator

- File and Printer Sharing.

2.3 Security Considerations

2.3.1 Mandatory Security Configuration

This section describes the steps you must take in order to secure your system. Detailed instructions for each step are provided at the appropriate point in the installation instructions. If you omit any of the steps in this section, some Unified CCDM functionality may not work properly.

- Configure Secure Sockets Layer (SSL) for the Unified CCDM web application (see section 6.2 "Configure SSL for Unified CCDM and Web Services" for instructions).
- Configure SSL for Web Services (see section 6.2 "Configure SSL for Unified CCDM and Web Services" for instructions).

2.3.2 Optional Security Configuration

This section describes the steps you may consider to secure your system. Detailed instructions for each step are provided at the appropriate point in the installation instructions.

To secure your system, you may consider the following steps :

- Disable anonymous sessions on all Unified CCDM servers (see section 3.4.1 "Disable Anonymous Sessions" for instructions). This prevents anonymous users from enumerating usernames and shares, and using this information to guess passwords or perform social engineering attacks. For more information, consult the Microsoft documentation http://technet.microsoft.com/en-us/library/dd349805(WS.10).aspx#BKMK_38 (link checked May 2013).
- Disable cached logins on all Unified CCDM servers (see section 3.4.2 "Disable Cached Logins" for instructions). This prevents attackers from accessing the cached login information and using a brute force attack to determine user passwords. If cached logins are disabled, windows domain users will be unable to log in if the connection to the domain controller is unavailable. For more information, consult the Microsoft documentation http://technet.microsoft.com/en-us/library/dd349805(WS.10).aspx#BKMK_27 (link checked May 2013).
- Disable DCOM on all Unified CCDM servers (see section 3.4.3 "Disable DCOM" for instructions). This makes the server less attractive to malware, which may be used to gain elevated privileges and compromise the system.

For more information, consult the Microsoft documentation http://technet.microsoft.com/en-us/library/dd632946.aspx (link checked September 2013).

- Enable mandatory Server Message Block (SMB) signing (see section 3.4.4 "Enable Mandatory SMB Signing for all Unified CCDM Servers" for instructions). This prevents “man in the middle” attacks that modify SMB packets in transit and ensures the integrity of file sharing and other network operations. For more information, consult the Microsoft documentation http://technet.microsoft.com/en-us/library/cc786681(v=ws.10).aspx (link checked August 2013).

Note

If you enable SMB signing, the server will not be able to communicate with a Microsoft network client unless that client agrees to perform SMB packet signing. So SMB signing will need to be enabled on every client machine in the cluster, including all clients running the web application.

- Disable SSL v2 on all App/Web Servers (see section 3.4.5 "Disable SSL V2"for instructions).This ensures that the latest version of SSL with the most recent security fixes is being used.

3 Windows and SQL Installation and Configuration

3.1 Windows Configuration

3.1.1 Firewalls

If your installation requires it, configure the firewall ports as described in section 2.2 "Firewall Configuration".

3.1.2 All Unified CCDM Servers

1. On each of the Unified CCDM servers in your installation:
   - configure the server to use the US English character set
   - configure Microsoft Terminal Services for remote configuration and support
   - in the Event Viewer, set the Application Log, Security Log and System Log to **Overwrite events as needed**.
2. Using the Windows Time Service, ensure the date and time are synchronized across all Unified CCDM servers. Unified CCDM will not be able to synchronize application data correctly between servers otherwise, and this may cause unexpected behavior.

3.2 SQL Server

3.2.1 Install SQL Server

Follow these instructions to install SQL Server on the server or servers that will be hosting the Unified CCDM database.

1. When presented with the SQL Server Installation Center select the **Installation** menu option from the left of the window.
2. Select **New installation or add features to an existing installation**.
3. The **Setup Support Rules** window will display validating the system for the installation of SQL Server 2008 R2. Once validation passes click **OK**.
4. Enter the product key for SQL Server 2008 R2 and click **Next**.

5. Read the license terms for SQL Server 2008 R2, if you agree with the terms select **I accept the license terms** and click **Next**.
6. You will be prompted to install the Setup Support Files. Click **Install**.
7. Once the Setup of Support Files is complete you will be presented with a summary of checks. Review the results and make any necessary changes. If you see a warning saying that Windows Firewall is enabled, you can safely ignore it. When you are satisfied, click **Next** to proceed.
8. Select the **SQL Server Feature Installation** option and click **Next**.
9. Select the following Instance Features:
    - **Database Engine Services**
        - **SQL Server Replication**
    - **Client Tools Connectivity**
    - **Management Tools – Basic**
    - **Management Tools – Complete**
10. Update the installation directories to install in the required locations. Click **Next**.
11. The installation rules are then checked. If any problems are reported, correct them, then click **Next**.
12. The Instance Configuration window is displayed. Select **Default Instance**, with an Instance ID of **MSSQLSERVER**. Update the Instance root directory to be installed on the required drive and click **Next**.
13. The Disk Space Requirements summary window is displayed. Click **Next**.
14. In the Server Configuration window, on the **Service Accounts** tab, set the following service configuration:
    - Locate the SQL Server Agent entry in the Service column, and set the corresponding Account Name to **NT AUTHORITY\SYSTEM** and the Startup Type to **Automatic**.
    - Locate the SQL Server Database Engine entry in the Service column and set the corresponding Account Name to **NT AUTHORITY\SYSTEM**.
15. In the Server Configuration window, on the **Collation** tab, ensure that the specified Database Engine collation is **Latin1_General_CI_AS**. If it is not, click **Customize**, and select a collation designator of **Latin1_General**, ensure that **Case-sensitive** is cleared and **Accent-sensitive** is selected, then click **OK**. When the collation is correct, click **Next** to proceed.
16. The Database Engine Configuration window is displayed.

- Select **Mixed Mode** authentication and enter a password for the **sa** user.
- In the Specify SQL Server administrators panel click the **Add Current User** button. Also add any other accounts that require administrator permissions to the Database, for example, Domain Admins, Service Accounts etc.
- Select the **Data Directories** tab. It is strongly recommended that the Temp DB directory and the Temp DB log directory are *not* located on the same drive as the Windows operating system. Make any required changes to the data directory locations.
- Click **Next** to proceed.

17. The Error Reporting window is displayed. Click **Next**.
18. The Installation Configuration Rules window is displayed and installation checks are performed. If any problems are reported, correct them. Click **Next**.
19. Review the installation summary and click **Install** to begin installing SQL Server 2008 R2.
20. Once the installation is complete click **Close**.
21. Locate and install SQL Server 2008 R2 Service Pack 2.

For a dual-sided deployment, repeat these steps on the Side B server.

3.2.2 Configure SQL Server Network Protocols

On the server or servers that will host the Unified CCDM Database, configure the SQL Server network protocols as follows:

1. Click **Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > SQL Server Configuration Manager** to open the SQL Server Configuration Manager.
2. In the left hand pane, expand **SQL Server Network Configuration** and click **Protocols for MSSQLSERVER**.
3. In the right hand pane right click on **Named Pipes**, select **Enable**, and click **OK** at the confirmation message.
4. In the right hand pane, right click on **TCP/IP**, select **Enable**, and click **OK** at the confirmation message.
5. In the left hand pane, click on **SQL Server Services**, then right click on **SQL Server (MSSQLSERVER)** and select **Restart** to restart the SQL Server process.
6. Close the SQL Server Configuration Manager window.

3.2.3 Configure Windows Firewall for SQL Server

By default the Windows Server 2008 R2 Firewall will not allow incoming traffic for SQL Server. If the Windows firewall is enabled, on the server or servers that will host the Unified CCDM Database, follow these steps to create a rule to allow SQL Server traffic:

1. Click **Start > All Programs > Administrative Tools > Server Manager**.
2. In the left hand pane, expand **Configuration > Windows Firewall with Advanced Security** and click **Inbound Rules**. A list of firewall rules is displayed.
3. In the **Actions** pane, click **New Rule**. The New Inbound Rule Wizard is displayed.
4. Select **Port** as the rule type and click **Next**.
5. Select **TCP** as the protocol and enter **1433** as the specific local port. **Click** Next. The Action options are displayed.
6. Choose **Allow the connection**. Click **Next**. The Profile options are displayed.
7. Select the profile options that are appropriate to your deployment and click **Next**.
8. Enter a name for the rule and click **Finish** to create the rule. The new rule appears in the list of inbound rules as an enabled rule.
9. Close the Server Manager window.

3.2.4 SQL Server Backup Guidelines

- Regularly backup the SQL Server databases and truncate transaction logs to prevent them becoming excessively large.
- Schedule backups for quiet times of the day.

3.3 User Accounts

3.3.1 Unified CCDM Service Accounts

Unified CCDM Services are installed to run under Windows system accounts (such as Network Service) by default.

Unified CCDM requires the following domain account to communicate between components.

SQL Agent User

SQL Server uses this account to replicate data between SQL Server databases. By default Unified CCDM expects the account name to be **sql_agent_user**, but you can specify a different name when Unified CCDM is installed.

Note
For single-sided installations, you can choose to allow Unified CCDM to create these accounts automatically as local accounts. But if you choose this option, then want to add a second side to your deployment later, you will need to reinstall the system.

To create the required accounts:

1. Using Active Directory, create the domain account **sql_agent_user** (or a name of your choice) with the following attributes:
   - Password never expires
   - User cannot change password.

3.4 Optional Security Configuration

3.4.1 Disable Anonymous Sessions

Note
This step is optional, although it is recommended for maximum security. See section 2.3 "Security Considerations" for more information.

This security setting applies to all Unified CCDM servers. There are several ways to configure this security setting. This section describes two possible ways.

One way is to use the Group Policy Editor to view the following path

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

then enable the setting

Network access: Do not allow anonymous enumeration of SAM accounts and shares.

Alternatively, you can update the registry directly as follows:

1. From the Windows Start Menu, click **Run**, then type **regedit**.
2. In the left hand pane, select the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa** node.

3. In the right hand pane, if the **REG_DWORD** value **restrictanonymous** is present, set it to 1, otherwise, create it and set it to 1. Click **OK**.
4. Close the registry editor.

3.4.2 Disable Cached Logins

Note
This step is optional, although it is recommended for maximum security. See section 2.3 "Security Considerations" for more information.

This security setting applies to all Unified CCDM servers. There are several ways to configure this security setting. This section describes two possible ways.

One way is to use the Group Policy Editor to view the following path

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

then set the following setting to **0**

Interactive logon: Number of previous logons to cache (in case domain controller is not available).

Alternatively, you can update the registry directly as follows:

1. From the Windows Start Menu, click **Run**, then type **regedit**.
2. In the left hand pane, select the **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Nt\CurrentVersion\Winlogon** node.
3. In the right hand pane, if the REG_SZ value **CachedLogonsCount** is present, set it to 0, otherwise, create it and set it to 0. Click **OK**.
4. Close the registry editor.

3.4.3 Disable DCOM

Note
This step is optional, although it is recommended for maximum security. See section 2.3 "Security Considerations" for more information.

This security setting applies to all Unified CCDM servers.

1. From the Windows Start Menu, select **Control Panel > Systems and Security > Administrative Tools > Component Services**.
2. Expand **Component Servers**, and then **Computers**. Right-click on **My Computer** and select **Properties**.

3. Select the **Default Properties** tab and clear **Enable Distributed COM on this computer**. Click **OK**, then **Yes** when asked to confirm that you want to update the DCOM Settings.
4. Close the Component Services dialog box, then reboot the server.

3.4.4 Enable Mandatory SMB Signing for all Unified CCDM Servers

Note
This step is optional, although it is recommended for maximum security. See section 2.3 "Security Considerations" for more information.

This security setting applies to all Unified CCDM servers.

1. From the Windows Start Menu, select **Control Panel > Systems and Security > Administrative Tools > Local Security Policy**. Navigate to **Local Policies > Security Options**.
2. In the right hand pane, click on **Microsoft network client: Digitally sign communications (always)**. Select **Enabled** and click **OK**.
3. In the right hand pane, click on **Microsoft network server: Digitally sign communications (always)**. Select **Enabled** and click **OK**.
4. Close the Local Security Policy dialog box.
5. On every client that needs to communicate with the Unified CCDMservers (including all clients running the Web UI), ensure that the following security options are set in the local security policy (select **Control Panel > Systems and Security > Administrative Tools > Local Security Policy** and navigate to **Local Policies > Security Options**):
   - **Microsoft network client: Digitally sign communications (always)**: ensure this is **Disabled** (the default value), unless other systems specifically require it to be enabled .
   - **Microsoft network client: Digitally sign communications (if server agrees)**: ensure this is **Enabled** (this is the default value).

3.4.5 Disable SSL V2

Note
This step is optional, although it is recommended for maximum security. See section 2.3 "Security Considerations" for more information.

On the App/Web Server:

1. From the Windows Start Menu, click **Run**, then type **regedit**.
2. In the left hand pane, select the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0** node.
3. If the registry key **Server** does not exist, right-click the **SSL 2.0** node, select **New > Key**, and create it.
4. Under the registry key **Server**, create a **DWORD** value named **Enabled** and set the value data to **00000000**.
5. Close the registry editor and reboot the server.

3.4.6 Disable Remote Access to Unified CCDM Servers

Unified CCDM servers can be administered remotely using tools such as Microsoft Terminal Services. Unified CCDM does not require remote access in order to work correctly, so for additional security you can disable remote access and use console access to administer the Unified CCDM servers.

4 Unified CCDM Installation

4.1 Before You Start

Note
The installation instructions assume that you are installing the product software on the C: drive. If you are installing the software on another drive, then where the instructions reference a specific drive, replace the reference to the C: drive with the drive you are using.

4.1.1 Installing Dual-Sided Systems

For dual-sided systems, perform a complete installation on the Side A servers, and then a complete installation on the Side B servers. It is recommended that you install the components in the order described here.

4.1.2 Recording Your Settings

During the installation procedure, there will be occasions where you need to record what settings you chose for later reference. It is recommended that you record the following information and store it in a secure location, for future reference.

System Setting	Value
Database Catalog Name	
sql_agent_user Password	
Cryptographic Passphrase	
Administrator Password	
Java.RMI.Hostname	
Unified CCE	
Application Name	
Application Key	
RMI Registry Port	
LocalPort	

4.2 The Unified CCDM Installer

4.2.1 About the Unified CCDM Installer

4.2.1.1 Starting the Installer

The Unified CCDM DVD contains the Unified CCDM Installer. To start the Installer, insert the DVD.

- If auto-run is enabled, a window opens automatically showing a list of Unified CCDM components that can be installed.
- If auto-run is disabled and you do not see the Installation Components screen, double-click the **autorun.bat** file located on the DVD to launch the Unified CCDM installer manually.
- If UAC has not been disabled, launch the installation manually by right-clicking on the **autorun.bat** file located on the DVD and selecting **Run as administrator** option.

Note

Some anti-virus software may state that the **autorun.hta** script file is malicious. Please ignore this message.

4.2.1.2 Installation Prerequisites

When you click on a component to install it, the installer displays a list of prerequisites for that component and checks that each prerequisite is present. As each prerequisite check completes, you will see a green tick (check successful) or a red cross (check failed).

Where possible, the Unified CCDM DVD includes redistributable packages for prerequisites, so if a prerequisite check fails, you can click on the link in the Unified CCDM installer to install the missing prerequisite. Once all the prerequisite software is installed, you can click on the component again, then click **Rerun** to rerun the tests.

When all the prerequisites display a green tick, you will be able to click **Install** to install the chosen component.

4.2.2 Install the Database Installer

This process does not install the database directly. It just installs the Database Installer which is then used to install the database.

On the Side A Database Server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see section 4.2.1 "About the Unified CCDM Installer").
2. Select **Database Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.
3. When all checks have passed, click **Install** to begin the Database Server Installation. The Setup window displays.
4. Click **Next** to go through each window in turn. You will need to enter the following details:
5. In the License Agreement window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.
6. In the Cryptography Configuration window:
   - **Passphrase.** Create a cryptographic passphrase of between 6 and 35 characters. This passphrase is used for encrypting and decrypting system passwords and must be the same for all servers in the Unified CCDMinstallation.
   - **Confirm Passphrase.** You will not be able to continue until the contents of this field are identical to the passphrase entered above.

Warning

The cryptographic passphrase is a vital piece of information and will be needed when installing later components and when adding or replacing servers in the future. Be sure to record and retain it.

If you are upgrading from a previous version of Unified CCDM, or adding a new server to an existing cluster, you must use the same cryptographic passphrase as was originally used. If you do not know the current cryptographic passphrase, **stop the installation immediately** and call your vendor support. If you continue the installation with a new passphrase you will be unable to access your existing data.

7. In the Configure Database window:
   - **Database Name**. Enter the name of the database catalog for Unified CCDM. By default this is **Portal**.
   - **Connect Using**. Select the login credentials you want to use:

- **Windows Authentication Credentials of Application**. This is the recommended option.
- **SQL Server Authentication using the login and password below**. This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your SQL Server Login Name and Password in the fields provided.

- **Click Next.**

8. In the Destination Folder window, you can click **Change** to change the location where the Database components are installed. It is not necessary to install all Unified CCDM components in the same location.
9. Click **Install** to install the Database Installer.

Note
During the Database Install Tool Installation, the J2SE pre-requisite will be automatically installed if it is not already present. You may see a Security Alert dialog box stating that 'Revocation Information for the security certificate for this site is not available'. If so, click **Yes** to continue.

10. To install or upgrade your database immediately after installing the Database Installer, select the **Launch Database Management Utility** check box at the end of the installation before clicking Finish.
11. Click **Finish**.

4.2.3 Install the Portal Database

To install the portal database:

1. If you selected the Launch Database Management Utility check box after installing the Database Installer, the database setup wizard will launch automatically. Otherwise you can launch the database installer from **Start > All Programs > Domain Manager > Database > Database Installer**.
2. Click **Next** to begin the installation.
3. In the **Select an Action to Perform** window, choose **Install a new database** You can maintain this database at a later date by running the installer again and selecting the appropriate option.
4. In the **SQL Server Connection Details** window:
   - **Server Name.** Enter the name of the machine that is to be the Database Server. This should normally be left as the default (local).

- **Database Name.** Enter or select the name of the database catalog that will be used for Unified CCDM. It is recommended that you use the default name of **Portal**. This should match the database catalog name specified when you installed the database installer. If not, you will see a warning message.
- **Connect Using.** Select the login credentials you want to use:
  - **The Windows account information I use to logon to my computer.** This is the recommended option.
  - **The SQL Server login information assigned by the system administrator.** Only select this option if you are using a database catalog on a different domain. For this option you must enter your SQL Server Login Name and Password in the fields provided.
- Click **Test Connection.** This makes sure the connection to the SQL Server is established. If the connection can be established, you will see the message 'Connection succeeded but database does not exist'.
- Click **Next** to continue.

5. In the **Setup Replication** window, if this database installation is not Side B of a replicated system, just click **Next**. If this database installation is Side B of a replicated system, select **Replicated Configuration** and set up the replication folder share as follows:
   - **Share Name** The name of the share for the ReplData folder. By default this is **ReplData**.
   - **Folder Path** The path of the ReplData folder. This is configured in SQL Server, and is by default **C:\Program Files\Microsoft SQL Server\MSSQL\repldata.**
   - **Click Next** when you have finished.
6. In the **Configure the Location of Data Files** window:
   a. Click **Select All**.
   b. Select **Set Initial Size to Max Size**.
   c. Click **Update**.
   d. Click **Select None**.
   e. Select each file in the File Group list in turn. For each:
      i. Refer to the table of file group names and sizes below and change the **Max Size** for the file group to the value shown for that file in the table.
      ii. Click **Update**.

iii. Clear the selection.

iv. Repeat for the next file in the File Group list.

f. Click **Next**.

File Group Name	Size
adminfilegroup	3310
adminindexfilegroup	830
dimfilegroup	11580
dimindexfilegroup	3310
factfilegroup	4100
factindexfilegroup	8210
fctauditfilegroup	1650
fctauditindexfilegroup	1852
fctcmsfilegroup	3310
fctcmsindexfilegroup	500
fctetlauditfilegroup	1650
fctetlauditindexfilegroup	250
fctfilegroup	1650
fcticmfilegroup	9920
fcticmindexfilegroup	1490
fctindexfilegroup	250
fctinfilegroup	1650
fctinindexfilegroup	250
fctivrfilegroup	8270
fctivrindexfilegroup	1240
fctmmfilegroup	3310
fctmmindexfilegroup	500

File Group Name	Size
fctwfmfilegroup	1650
fctwfmindexfilegroup	250
logfilegroup	17575
primaryfilegroup	6620
secfilegroup	3310
secindexfilegroup	830
stagingfilegroup	8270
stagingindexfilegroup	3310
sumcmsfilegroup	6620
sumcmsindexfilegroup	990
sumfilegroup	290
sumicmfilegroup	6620
sumicmindexfilegroup	990
Sumindexfilegroup	290
suminfilegroup	6620
suminindexfilegroup	990
sumivrfilegroup	6620
sumivrindexfilegroup	990
summmfilegroup	6620
summmindexfilegroup	990

7. The **Configure SQL Server Agent Service Identity** window sets up a user account that is used by SQL Server for replication:
   - **Account Type** The type of user account that will be used. For a distributed installation, this must be **Domain**.
   - **User Name** The name of the SQL agent user account. This defaults to **sql_agent_user**. If you have not already created this account, set it up now as described in section 3.3 "User Accounts". If you used a different name when setting up the account, enter that name instead. If

- you have specified a domain user, you will need to prefix the user name with the domain name, followed by a backslash. For example if the SQL agent user belongs to the **UCCDMDOM** domain then enter **UCCDMDOM\sql_agent_user**.
- **Automatically create the user account if missing** For a single-sided system, you can optionally select this check box and create the required user automatically. But if you select this option and need to add a second side in future, you will need to reinstall the system.
- **Password** If you are using an existing SQL agent user account, enter the password for that account. Otherwise, if you have a single-sided system and are creating the account automatically, create a password for the new user, conforming to the complexity requirements for your system.
- **Confirm Password** You will not be able to continue until the contents of this field are identical to the password entered above.
- Click **Next**.

8. In the **Ready to install the Database** window, click **Next** to begin installation. Installation will take several minutes.
9. Click **Close** to close the installer.

4.2.4 Install the App/Web Server

Install the new App/Web Server components. In most installations, the App/Web Server component should be installed on a different physical machine to the Database Server component.

On the Side A App/Web Server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see section 4.2.1 "About the Unified CCDM Installer").
2. Select **App/Web Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.
3. When all checks have passed, click **Install** to begin the App/Web Server installation. The **Domain Manager: Application Server Component** window displays.
4. Click **Next** to go through each window in turn. You will need to enter the following details:
5. If the Domain Manager: Application Server Components Dialog is displayed, click **Install** to install the additional required components.

6. If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.5 Framework is complete, restart the server to continue the installation of the App/Web Server.
7. In the **License Agreement** window:
   - **I accept the terms in the license agreement**. You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.
8. In the **Cryptography Configuration** window:
   - **Passphrase**. Enter the cryptographic passphrase you created during installation of the Database Server component.
   - **Confirm Passphrase**. You will not be able to continue until the contents of this field are identical to the passphrase entered above.
   - Click **Next** to continue.

Warning!
You must use the same cryptographic passphrase for all servers in theUnified CCDM installation. If you do not know the cryptographic passphrase, **stop the installation immediately** and contact your vendor support. If you continue the installation with a new passphrase the installation will not work.

9. In the **Destination Folder** window, you can click **Change** to change the location that the App/Web Server components are installed to. Click **Next** to continue.
10. In the **Configure Database** window:
    - **SQL Server Name**. Enter the host name or IP Address of the server hosting the Unified CCDM database. The default name of **localhost** is only valid if you are installing this component on the Database Server. Otherwise, specify the name of the Database Server. For a dual-sided deployment enter the name of the Side A Database server when installing the Side A components and enter the name of the Side B Database Server when installing the Side B components.
    - **Catalog Name**. Enter or select the database catalog name you specified when installing the Database Server component. If you used the default value, this will be **Portal**.
    - **Connect Using**. Select the login credentials you want to use:
      - **Windows authentication.** This is the recommended option.

- **SQL Server authentication.** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter a SQL Server Login Name and Password in the fields provided.

- Click **Next** to continue.

11. Click **Install**.
12. When the installation has completed, click **Finish**.

Note
The machine will restart once the installation is complete.

4.2.5 Install the Second Side (Replicated Systems Only)

For replicated systems this installation needs to be repeated for Side B. It is recommended that you complete the Side A installation of all components before installing Side B.

4.3 Support Tools

4.3.1 About the Support Tools

Unified CCDM includes support for integration with the Cisco Real Time Monitoring Tool (RTMT). This allows remote monitoring and support for your Unified CCDM installation. To use RTMT you need to install the Diagnostic Framework component of Unified CCDM which provides access to relevant support APIs. These APIs can be used by the RTMT for gathering trace levels, log files etc.

4.3.2 Install the Diagnostic Framework

1. To install the Diagnostic Framework component, start the Unified CCDM Installer, click **Support Tools** and select **Diagnostic Framework**. The **Domain Manager: Diagnostic Framework InstallShield Wizard** window displays.
2. Click **Next** to go through each window in turn. You will need to enter the following details:
3. In the **License Agreement** window:

   - **I accept the terms in the license agreement**. You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.

- Click **Next**.

4. In the **Select Certificate** window, select the type of certificate installed with the Diagnostic Framework.
   - **Self Signed**. A new certificate will be generated by the installer. This type of certificate should be used only for lab or test deployments.
   - **Trusted Certificate**. An existing certificate issued by a valid certificate server will be associated at a later date. This option should be used for production deployments.
   - Click **Next**.
5. In the wsmadmin Password Information window, enter the password for the **wsmadmin** user that will be created to access the Unified System CLI tool. Enter your chosen password again to confirm it. Click **Next**.
6. Click **Install**.
7. When the installation is completed, click **Finish**.

The installation of the Diagnostic Framework component is now complete.

5 Unified CCDM Configuration

5.1 About Unified CCDM Configuration

Unified CCDM will normally be hosted on multiple servers for performance and data security. This chapter describes how to configure the server cluster and perform data replication.

This section describes the following steps:

- configuring Unified CCE Admin Workstations
- configuring Unified CCE for provisioning
- configuring the Unified CCDM cluster
- configuring replication
- configuring Unified CVP media file upload.

5.2 Configure Unified CCE Admin Workstations

Note
If Unified CCDM uses SQL Server Authentication to connect to Unified CCE no configuration of the AWDB is required. However, the SQL login used for the connection must have the appropriate permissions on the AWDB and the HDSDB.

If SQL Server Authentication is not in use for Admin Workstation (AW) SQL connections then the following configuration is required:

1. Login to the AW as a user with local administrative privileges.
2. Open the SQL Server Management Studio, by clicking **Start > All Programs > Microsoft SQL Server > SQL Server Management Studio** Connect to the server.
3. Open up the **Security** folder, and right-click **Logins**.
4. Select **New Login** from the drop-down list. The Login – New window displays.
5. Add SQL logins for the Network Service accounts of each server hosting Unified CCDM (Database Servers and App/Web Servers), by filling in the fields as follows:
    - **General** page:

- **Login Name**: Enter the machine name in the form **<DOMAIN>\<MACHINENAME>$**, for example **ACMEDOM\ACMEWEBA$**. This configures access for the NETWORK SERVICE account from the Unified CCDM server.
- **Authentication**: Select Windows Authentication unless connecting to a server on a different domain

- **User Mapping** page:
  - **Users mapped to this login**. Select AWDB and HDSDB.
  - **Database role membership for**. For AWDB and HDSDB, select **Public** and **db_datareader**.

6. Click **OK**.

5.3 Configure Unified CCE Provisioning

5.3.1 About Provisioning Configuration

Cisco Unified Contact Center Enterprise (Unified CCE) components must be correctly configured before Unified CCDM can connect to them for Provisioning.

For each Unified CCE instance that Unified CCDM Resource Management connects to, certain essential criteria must be met:

- Unified CCDM Resource Management uses Cisco ConAPI for the Provisioning connections: this interface requires that all connections are made to a Primary Distributor AW. If the AW is dual-sided, both sides must be Primary Distributors.
- Multiple Unified CCE instances can be supported, but each requires a distinct primary Distributor AW to connect to:
  - ConAPI only supports connection to one Application Instance on each physical server. You must therefore have a separate physical AW distributor for each instance.
  - Parent/Child AW configurations are supported as multiple instances in Unified CCDM.

Note
Please contact your vendor support if you have any queries about this configuration.

- If your deployment will include resource management, you must set up the ConAPI application instance and the CMS server on your Unified CM and Unified CCE instances.

5.3.2 Set Up ConAPI

To set up the ConAPI application instance, you must run Configuration Manager on the Unified CCE Admin Workstation (AW) as follows:

1. Open Configuration Manager. This can normally be done from **Start > Program Files > Cisco Unified CCE Tools > Administration Tools > Configuration Manager**

> **Note**
> If you are connecting to the Unified CCE server using Remote Desktop, you will need to set the **/admin** switch in order to run Configuration Manager.

2. Under **Tools > List Tool**s you will find the **Application Instance List**. Double-click this to open it.
3. Click **Retrieve** to display the list of configured application instances. You can use an application instance from this list for Unified CCDM or create a new one. To create a new application instance, click **Add**, and enter the following details:
   - **Name** A unique name to be used for the application instance.
   - **Application Key** A password to be used by Unified CCDM to connect. This may be between 1 and 32 characters.
   - **Confirm Application Key** Ensure that no typographical errors were made while choosing the application key.
   - **Application Type** Select **Cisco Voice.**
   - **Permission Level** Give the application full read/write permissions.
4. Record these details for use during the configuration of the cluster.
5. Click **Save** and then click Close.

5.3.3 Set Up the CMS Server

Ensure that the CMS Server(s) are set up correctly on each Unified CCE.

Firstly, check that the CMS Node option was selected when the Admin Workstation was configured. You can determine if this was the case by looking for a **cmsnode** and a **cms_jserver** process running on the Unified CCE.

If these processes are not present, set the CMS Node option on the Unified CCE. See the *Cisco Unified CCE Installation Guide* for details on how to do this.

A new application connection must be defined on each configured Unified CCE instance for each Database Server (this connection is used by the Data Import Server component). This ensures that in a dual-sided system, the alternate side can also connect to the Unified CCE in a failover scenario. To do this:

1. On the Unified CCE being configured, go to **Start > Program Files > Cisco Unified CCE Tools > Administration Tools > CMS Control** on the Unified CCE being configured. This opens the CMS control console.
2. Click **Add** to the right hand side of the window to launch the Application Connection Details window and fill in the fields as follows:
    - **ICM Distributor AW link**, This should be the name of the Unified CCDM Database Server, all in capital letters, with 'Server' appended, for example, **ProductDBServer**.
    - **ICM Distributor AW RMI registry port,** This is the port on the Unified CCE AW for the Unified CCDM Provisioning service to connect to. This will usually be 2099, however if the Unified CCDM Provisioning service is connecting to multiple Unified CCE instances each should use a different port.
    - **Application link**, This is the name of the Unified CCDM Database Server, all in capital letters, with 'Client' appended, for example, **ProductDBClient**.
    - **Application RMI registry port**, This is the port on the Unified CCDM Database Server for the Unified CCE AW to connect to. For convenience, this should be the same as for the ICM Distributor AW RMI registry port. Each Unified CCE AW must connect to a different port on the Database Server. You should record this information for future use.

Note
Each Unified CCE that Unified CCDM will be provisioning must use a unique port on the Database Server.

    - **Application host name**. The server name, for example, **ProductAppServer**
3. Click **OK**, and **OK** again to cycle the CMSJServer, save your changes and close the CMS control console.

5.4 Configure the Unified CCDM Cluster

5.4.1 About Cluster Configuration

Use the Cluster Configuration tool in the Unified CCDM Integrated Configuration Environment (ICE) to:

- configure the servers in the Unified CCDM cluster (the Unified CCDM servers, Unified CCEs and Unified CMs)
- set up the equipment mappings between remote tenants and Unified CCDM resources.

Follow the instructions below to configure your system when you first install it. For more information about using the ICE tools to modify your system configuration at a later date, see the Integrated Configuration Management section of the *Administration Guide for Cisco Unified Contact Center Domain Manager*.

5.4.2 Start ICE Cluster Configuration

To start ICE, on the Side A Database Server:

1. Go to **Start > All Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment**.
2. The **Database Connection** window is displayed. In this window, set:
   - **Server Name**. This option defaults to the current machine.
   - **Database Name**. Select the Unified CCDM database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
   - **Authentication**. Select Windows Authentication.
3. Click **OK** to open ICE. The ICE Cluster Configuration tool starts by default.
4. In the ICE Cluster Configuration tool, select the **Setup** tab in the left hand pane. This displays a series of wizards to set up the servers.

The following sections explain how to use each of the wizards.

5.4.3 Set Up Unified CCDM Servers

The Setup Unified CCDM Servers wizard configures the servers on which Unified CCDM components are installed. The wizard guides you through the steps to configure all Unified CCDM components based on your chosen deployment model.

Note
The exact windows displayed by the wizard may depend on the options you choose as you complete each step below.

To set up the Unified CCDM servers:

1. In the ICE Cluster Configuration tool, select the **Setup** tab and click **Setup UCCDM Servers** to start the wizard. Click **Next** to go through each window in turn.
2. In the **Select Deployment Type** dialog box select your chosen deployment type.
3. In the **Configure Redundancy** dialog box select whether you would like to configure a single-sided or a dual-sided system. Click **Next**.
4. If you are performing a two tier deployment then you will be asked to enter the number of web servers for each side. Enter the number of app/web servers on each side of your deployment. Dual-sided configurations must have an equal number of app/web servers on each side. Click **Next**.
5. In the **Configure Servers** dialog boxes, enter the server names for each of the Unified CCDM servers. The number of dialog boxes and servers to specify will depend on the deployment options you chose above.
6. In each dialog box, enter the following, then click **Next**:
   - **Primary Server**
     - **Server Name**. This is the non-domain qualified machine name.
     - **Server Address**. This defaults to Server Name. This can be changed to an IP Address or a domain qualified name of the server.
   - **Secondary Server**:
     - If you chose a dual-sided setup, provide the corresponding details for the Side B server.
7. Click **Next** and enter the relevant server information for each Unified CCDM server until you reach one of the following dialog boxes: **Primary Database Administrator Login**, **Secondary Database Administrator Login** or **Configure Relational Database Connection**.

Note
The Primary and Secondary Database Administrator Login dialog boxes are only shown if the database user you specified when you started ICE does not have sufficient permissions to create new SQL Server users and grant permissions to them. If the current database user has sufficient permissions on a server then you will not see the Database Administrator Login dialog box for that server.

8. If the **Primary Database Administrator Login** dialog box is shown, provide details of a SQL Server user account on the primary database server that has sufficient permissions to create new SQL Server users and grant permissions to them. This account is used to set up the users and permissions required by Unified CCDM to connect the Unified CCDM services to the portal database. This account is only used during system setup.
    - **Authentication**. Select the authentication mode for this user.
        - **Windows Authentication**. Select this option to use the currently logged in Windows domain user.
        - **SQL Authentication**. Select this option to use a specific SQL Server user. Either accept the default **sa** user (created when the Unified CCDM database was installed, and which does have sufficient permissions) or enter another SQL Server user, then specify the password.
    - Click **Next**.
9. If you have specified a dual-sided installation, and the **Secondary Database Administrator Login** dialog box is shown, follow the instructions in step 8. to provide details of a database user account with sufficient privileges on the secondary database server.
10. In the **Configure Relational Database Connection** dialog box enter the connection details to be used by each Unified CCDM server to connect to the Unified CCDM portal database:
    - **Catalog**. This is the name of the Unified CCDM database. The default is **Portal**.
    - **Authentication**. Select the authentication mode to use to connect to the Unified CCDM database.
        - **Windows Authentication**. The recommended authentication mode. If this mode is selected, each Unified CCDM service will connect to the portal database using the Windows account under which the service is running (by default, all Unified CCDM services run under the Network Service account).

- **SQL Authentication**. Only select this option if you are using a Database Server on a different domain. For this option you must enter the SQL Server username and password in the fields provided.

- Click **Next**. If you selected SQL Authentication and the specified account does not yet exist, you will be prompted to create it.

11. The **Deployment Summary** dialog box summarizes the choices you have made. If you want to print the deployment summary, click the **Print** button below the summary list.
12. Check the deployment details, and if you are satisfied, click **Next**.
13. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.
14. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu.

5.4.4 Configure Cisco Unified CCE Servers

The Configure Cisco Unified CCE Servers wizard configures Cisco Unified CCE instances. This wizard guides you through the steps to:

- add a new Cisco Unified CCE instance to the deployment
- update an existing Cisco Unified CCE instance in the deployment
- remove an existing Cisco Unified CCE instance from the deployment.

5.4.4.1 Unified CCE Deployment Models

Unified CCE offers a number of different deployment models depending on customers requirements. Unified CCDM supports the following Unified CCE deployments:

- Administration Server and Real-time Data Server (AW)
- Configuration-only Administration Server
- Administration Server and Real-Time and Historical Data Server (AW-HDS)
- Administration Server, Real-Time and Historical Data Server, and Detail Data Server (AW-HDS-DDS)

5.4.4.2 Unified CCDM Connection Requirements

To configure the different deployment models Unified CCDM requires a connection to:

- Unified CCE real-time AWDB for data import

- Unified CCE AW for Unified CCDM Provisioning Server requests.

5.4.4.3 Configuring the Servers

Note
This wizard attempts to connect to Cisco Unified CCE Servers using SQL Connection. The connection credentials should be known prior to starting the configuration.

If you require resource management (provisioning), you will also need to know the login details for a user with appropriate access to the Unified CCE used for provisioning. On the domain controller, this user must be in the domain security group **<Server>_<UCCEInstance>_Config**, where <*Server*> is the name of the server running Unified CCE and <*UCCEInstance*> is the name of the Unified CCE Instance on this server.

To configure the Cisco Unified CCE servers:

1. In the ICE Cluster Configuration tool, select the **Setup** tab and click **Configure Cisco Unified CCE Servers** to start the wizard. Click **Next** to go through each window in turn.
2. In the **Select Task** dialog box select the action. The options are:
   - Add a new instance
   - Modify an existing instance
   - Remove an existing instance.

Note
The Modify and Remove options are only enabled when at least one Cisco Unified CCE has already been configured.

3. In the **Specify Resource Name** dialog box, specify the name for the instance being configured. You can use the default name or choose another name.
4. In the Select Required Components dialog box, select all the required components in the deployment.
   - **Admin Workstation**. Select this component for all configurations.
   - **ConAPI Server (Provisioning)**. Select this component if you require resource management.
5. In the **Configure Redundancy** dialog box, select whether you want to configure a single-sided or a dual-sided setup.
6. In the **Configure AW Server** dialog box, enter the following:
   - **Primary Server**:

- **Sever Name**. This is the non-domain qualified machine name where the Admin Workstation and ConAPI components are deployed.
- **Server Address**. This defaults to Server Name. This may be changed to an IP Address or a domain qualified name of the server.

- **Secondary Server**:
  - If you chose a dual-sided setup, provide the corresponding server details for the Side B server.

7. In the **Configure Connection Details** dialog box, enter the authentication details to connect to the Admin Workstation database.
   - **Windows Authentication.** This is the default recommended authentication mode.
   - **SQL Authentication**. If this mode is chosen then specify the SQL Server user name and the corresponding password to connect to the databases.
8. In the **Select Unified CCE Instance** dialog box select the AW instance to be used in the deployment. Click **Next**.
9. If you selected the ConAPI Server (Provisioning) option above then you will see the following dialog boxes:
10. In the **Configure Primary Unified Config Web Service** dialog box (only shown you selected the ConAPI Server (Provisioning) option above, and the Unified CCE instance is running Unified CCE version 9.0 or later), enter the following details
    - **URL**. This is the auto-generated URL of the primary unified config web service on the Unified CCE
    - **User Name**. This is a username with appropriate access to the Unified CCE that the web service is running on. This user must be in the domain security group **<Server>_<UCCE-Instance>_Config**, where <*Server*> is the name of the server running Unified CCE and <*UCCE-Instance*> is the name of the Unified CE Instance on this server. For Unified CCE version 9.0(1) or 9.0(2), enter the username as **<domain>\<user>** and for Unified CCE version 9.0(3) or later, enter the username as **<user>@<domain>**, where <user> is the Unified CCE username, and <domain> is the name of the domain.
    - **Password**. This is the password for the user.

11. In the **Configure Primary ConAPI RMI Ports** dialog box (only shown if you selected the ConAPI Server (Provisioning) option above) enter the following ConAPI details:
    - **Local Registry Port.** This is the port on the Unified CCE for the Unified CCDM Provisioning service to connect to. This will usually be 2099.
    - **Remote Registry Port.** This is the port on the Unified CCDM Database Server for the Unified CCE to connect to. This will usually be 2099.
    - **Local Port.** This is selected as the designated port for live provisioning traffic between the Unified CCE and Unified CCDM servers. It must be uniquely assigned for each Unified CCE and any firewalls between the CICM and Unified CCDM server must be configured to allow both-way traffic on this port.

Note
If dual-sided setup is being configured you will need to provide these details for the Secondary (Side B) server in the next window.

- In the **Configure ConAPI Application Instance** dialog box enter the following details:
    - **Application Name.** The name of the application to be used for provisioning Unified CCE from Unified CCDM. Specify the name of the application you configured in section 5.3.2 "Set Up ConAPI" Credentials.
    - **Application Key.** Use the password for the application you specified above.
- In the **Multi Media Support** dialog box, select **Yes** if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance to provide support for non-voice interactions. The default is No.
- In the **Purge On Delete** dialog box select **Yes** if you want to purge items from Unified CCE automatically when they are deleted from Unified CCDM. The default is Yes.
- In the **Supervisor Active Directory Integration** dialog box select **Yes** if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors. The default is No. If you select Yes then you will be prompted to provide Active Directory information so that Windows user accounts can be listed.

12. In the **Configure Linked Unified CM Servers** dialog box select the configured Unified Communications Manager servers that the Unified CCE being configured is capable of routing calls to.

Note
The Configure Linked Unified CM Servers window only appears if at least one Unified CM server is already configured. You will be able to link the Unified CM servers to the Unified CCE from the Unified CM Configuration Wizard. You may also modify the Unified CCE once the Unified CM servers are configured and link the Unified CM later.

13. The **Summary** dialog box summarizes the details of the Unified CCE being configured and the settings you have chosen. If you want to print the summary, click the **Print** button below the summary list.
14. Check the details, and if you are satisfied, click **Next**.
15. A confirmation message is displayed to indicate that the wizard has completed successfully. Click Exit to close the wizard.
16. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu.

5.4.5 Configure Cisco Unified CM Servers

The Configure Cisco Unified CM Servers wizard configures Cisco Unified CM instances. This wizard guides you through the steps to:

- add a new Cisco Unified CM instance to the deployment
- update an existing Cisco Unified CM instance in the deployment
- remove an existing Cisco Unified CM instance from the deployment.

To configure the Cisco Unified CM servers:

1. In the ICE Cluster Configuration tool, select the **Setup** tab and click **Configure Cisco Unified CM Servers** to start the wizard. Click **Next** to go through each window in turn.
2. In the **Select Task** dialog box, select the action. The options are:
    - Add a new instance
    - Modify an existing instance
    - Remove an existing instance

Note
The Modify and Remove options are only enabled when at least one Cisco Unified CM has already been configured.

3. In the **Specify Resource Name** dialog box, specify a name for the instance being configured. You can use the default name or choose another name.
4. In the **Configure Unified CM** Servers dialog box enter the following:
    - **Primary Server**
        - **Sever Name**. This is the non-domain qualified machine name where the Cisco Unified CM components are deployed.
        - **Server Address**. This defaults to Server Name. This can be changed to an IP Address or a domain qualified name of the server.

Note
When configuring a Unified CM Cluster ensure that only the publisher of the cluster is configured.

    - **Secondary Server**: This option is always disabled.
5. In the **Select Version** dialog box select the version of Unified CM being configured from the drop-down list.
6. In the **Connection Details** dialog box enter the following details:
    - **URL**. This is used to access the Unified CM AXL interface. The default is the default URL for the Unified CM version that has been selected. It is recommended that you use the default URL.
    - **User Name**. This is the name of the Unified CM Administrator user. This is the user name that the Unified CCDM components use when connecting to the Unified CM AXL web service.
    - **Password**. This is the Unified CM Administrator user's password.
7. In the **Configure Linked Unified CCE Servers** dialog box select the configured Cisco Unified CCE servers that can route calls to the Unified CM being configured.

Note
The list will be empty if no Cisco Unified CCE servers have been configured. You will be able to link the Unified CM server to the Unified CCEs from the Cisco Unified CCE Configuration Wizard. You can also modify the Unified CM once the Cisco Unified CCE servers are configured and link the Unified CM later.

8. The **Summary** dialog box summarizes the details of the Unified CM being configured and the settings you have chosen. If you want to print the summary, click the **Print** button below the summary list.
9. Check the details, and if you are satisfied, click **Next**.
10. A confirmation message is displayed to indicate that the wizard has completed successfully. Click Exit to close the wizard.
11. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu.

5.4.6 Configure Cisco Unified CVP Servers Wizard

The Configure Cisco Unified CVP Servers wizard configures Cisco Unified CVP server clusters. A Cisco Unified CVP server cluster consists of a Unified CVP Operations Console and, optionally, one or more call servers.

This wizard guides you through the steps to:

- add a new Cisco Unified CVP cluster instance to the deployment
- update an existing Cisco Unified CVP cluster instance in the deployment
- remove an existing Cisco Unified CVP cluster instance from the deployment.

To configure a Cisco Unified CVP server cluster:

1. In the ICE Cluster Configuration tool, select the **Setup** tab and click **Configure Cisco Unified CVP Servers** to start the wizard. Click **Next** to go through each window in turn.
2. In the **Select Task** dialog box, select the action. The options are:
   - Add a new instance
   - Modify an existing instance
   - Remove an existing instance.

   The Modify and Remove options are only enabled when at least one Cisco Unified CVP cluster instance has already been configured.
3. In the **Specify Unified CVP Operations Console Resource Name** dialog box, specify a name for the Unified CVP operations console.

4. In the **Select Version** dialog box, specify the version of Unified CVP that is running on the CVP cluster you are configuring.
5. In the **Configure Unified CVP Operations Console** dialog box, enter the following:
   - **Primary Server**:
     - **Sever Name**. This is the non-domain qualified machine name where the Cisco Unified CVP Operations Console is deployed.
     - **Server Address**. This defaults to Server Name. You can change this to an IP Address or a domain qualified name of the server.
   - **Secondary Server**: This option is always disabled.
6. In the **Configure Primary Unified Config Web Service** dialog box (only shown when the selected Unified CVP version is 10.0 or later), enter the following details:
   - **URL**. This is the auto-generated URL of the primary unified config web service on the Unified CVP cluster.
     - **User Name**. This is a username with appropriate access to the Unified CVP that the web service is running on.
     - **Password**. This is the password for the user.
7. In the **Select Number of Call Servers** dialog box, specify the number of CVP call servers in the CVP cluster.

Note
All CVP call servers must be on the same Unified CCE as the Unified CVP operations console.

8. If you specified at least one call server:
   a. In the **Specify Unified CVP Call Server 1 Resource Name** dialog box, enter a name for the call server.
   b. In the **Configure Unified CVP Call Server 1** dialog box, enter the following:
   - **Primary Server**:
     - **Sever Name**. This is the non-domain qualified machine name of the Cisco Unified CVP call server.
     - **Server Address**. This defaults to Server Name. You can change this to an IP Address or a domain qualified name of the server.
   - **Secondary Server**: This option is always disabled.

9. If you specified more than one call server, repeat step 8. to provide the details for the each of the remaining call servers.
10. The **Summary** dialog box summarizes the details of the Unified CVP cluster being configured and the settings you have chosen.
11. Check the details, and if you are satisfied, click **Next**.
12. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.
13. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu.

5.4.7 Configure Avaya CMS Servers Wizard

The Configure Avaya CMS Servers wizard configures Avaya CMS database servers.

This wizard guides you through the steps to:

- add a new Avaya CMS server to the deployment
- update an existing Avaya CMS server instance in the deployment
- remove an existing Avaya CMS server instance from the deployment.

To configure a Avaya CMS server:

1. In the ICE Cluster Configuration tool, select the **Setup** tab and click **Configure Avaya CMS Servers** to start the wizard. Click **Next** to go through each window in turn.
2. In the **Select Task** dialog box, select the action. The options are:
   - Add a new instance
   - Modify an existing instance
   - Remove an existing instance.

   The Modify and Remove options are only enabled when at least one Avaya CMS server instance has already been configured.
3. In the **Specify Resource Name** dialog box, specify a name for the Avaya CMS resource.
4. In the **Select Version** dialog box, specify the version of Avaya CMS that is running on the Avaya CMS server you are configuring.
5. In the **Configure Avaya CMS Database Server** dialog box, enter the following:

- **Primary Server**:
  - **Sever Name**. This is the non-domain qualified machine name where the Avaya CMS database server is deployed.
  - **Server Address**. This defaults to Server Name. You can change this to an IP Address or a domain qualified name of the server.
- **Secondary Server**: This option is always disabled.

6. In the **Configure Avaya CMS Database Credentials** dialog box, enter the following:
   - **Instance Name**: This is the Informix instance name for the Avaya CMS Database.
   - **Protocol**: This should be set to the recommended default of **onsoctcp**.
   - **Service**: This is the service port used to connect to the Avaya CMS Informix database. The default is **1526**. However this may be different for some installations.
   - **User Name**: The user name to connect to the Avaya CMS Informix database.
   - **Password**: The password for the user specified above.
   - **Catalog**: The Avaya CMS database catalog. In most cases the default is **cms**.
7. In the **Select Mediator Server** dialog box, select the Mediator Server to use to import data from the Avaya CMS server.
8. The **Summary** dialog box summarizes the details of the Avaya CMS server being configured and the settings you have chosen.
9. Check the details, and if you are satisfied, click **Next**.
10. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.
11. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu.

5.4.8 Create and Map Tenants

5.4.8.1 About Creating and Mapping Tenants

The Equipment Mapping tab of the ICE Cluster Configuration tool allows you to create new tenants and folders and map them to the contact center equipment you have just configured. Use this tool to:

- create the Unified CCDM folder structure for your deployment

- specify the rules for importing resources into your Unified CCDM folder structure from the contact center equipment (for example, Unified CCE, Unified CM).

5.4.8.2 Creating Tenants and Folders

To create a Unified CCDM tenant:

1. In the ICE Cluster Configuration tool, select the **Equipment Mapping** tab. In the center pane, right click on the root node and select Add Tenant.
2. In the **Name** field enter the name of the tenant, and optionally, in the **Description** field, enter a description.
3. Select **File > Save** to save your changes. If you exit the tool without saving your changes you will be asked whether you want to save your changes when you exit the tool.

To create a Unified CCDM folder:

1. In the ICE Cluster Configuration tool, select the **Equipment Mapping** tab. In the center pane, right click on the folder tree at the location where you want to add the folder and select Add Folder.
2. In the **Name** field enter the name of the folder, and optionally, in the **Description** field, enter a description.
3. Select **File > Save** to save your changes. If you exit the tool without saving your changes you will be asked whether you want to save your changes when you exit the tool.

5.4.8.3 Creating an Equipment Mapping

To create an equipment mapping between a tenant or folder and the contact center equipment:

1. In the ICE Cluster Configuration tool, select the **Equipment Mapping** tab. In the folder tree, select the tenant or folder into which you want to import the resources from the contact center equipment.
2. In the adjoining pane select the check box or check boxes next to each item of contact center equipment that you want to associate with the selected folder or tenant.
3. Highlight each selected item of contact center equipment in turn, and, in the right hand pane, select one of the following check boxes:
   - **Default Import Location**. All the resources imported from the highlighted contact center equipment will be placed in the selected folder or tenant in Unified CCDM.

- **Remote Tenant Mapping**. All resources imported from the highlighted contact center equipment associated with the selected remote tenant will be placed in the selected folder or tenant in Unified CCDM. If you select this option, also select a remote tenant from the drop-down list.

Note
If Remote Tenant Mapping is selected then any resources on the contact center equipment that are not associated with the selected remote tenant will be placed in the source equipment subfolder under the Unallocated folder.

4. Select **File > Save** to save your changes. If you exit the tool without saving your changes you will be asked whether you want to save your changes when you exit the tool.

5.5 Replication

5.5.1 About Replication

5.5.1.1 About the Replication Manager

In a dual-sided deployment, use the ICE Replication Manager to configure and monitor database replication between publisher and subscriber databases. The publisher is usually on Side A, but it may occasionally be necessary to configure Side B as the publisher.

The Replication manager has two modes,setup and monitor. Setup is used to configure or disable replication and monitor is used to monitor the status of a configured replication.

When your system is first installed you should:

- configure replication as described in section 5.5.2 "Configure Replication"
- monitor replication as described in section 5.5.3 "Monitor the Replication Snapshot"

For more information about using the ICE Replication Manager to manage replication at a later date, see the Integrated Configuration Management section of the *Administration Guide for Cisco Unified Contact Center Domain Manager*.

5.5.1.2 About The Snapshot Process

When replication is configured, the existing data from the publisher database is pushed to the subscriber database. This is referred to as the *snapshot* process.

The snapshot process takes a variable time depending in the amount of data contained in the publisher database. For new deployments where the import from Unified CCE or Unified CM has not yet been performed, this is likely to be a few minutes. On large deployments where Unified CCE or Unified CM resources have already been imported to the publisher database this could take a lot longer.

Note
The subscriber database cannot be used until the snapshot process has completed.

5.5.1.3 About Replication Publications

When replication is configured the following publications are set up (assuming you have used the default database name of **Portal**):

- **[Portal]: BasePubWin**
- **[Portal]: BaseSubWin**
- **[Portal]: NonQueued**

Each of these publications contains a series of tables which are replicated between the publisher and subscriber as part of the snapshot process. **[Portal]: BaseSubWin** is the largest publication and will take the longest for the snapshot process to complete. Each of the publications will migrate through the following steps during the snapshot process :

- **Pre** preparation
- **Sch** schema
- **Data copy**
- **Dri** referential integrity
- **Post Snapshot Commands**

You can monitor the progress of the snapshot process using the Monitor tab which is automatically shown after the replication configuration has completed.

5.5.2 Configure Replication

Note
The user running Replication Manager must have administrator permissions in both Windows and SQL Server, for both the publisher and subscriber Database Servers.

Before configuring replication you should have already configured Unified CCDM in dual-sided mode using the Cluster Configuration tool as described in section 5.4 "Configure the Unified CCDM Cluster".

To configure replication, on the Database Server that will be the publisher:

1. Go to **Start > All Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment**.
2. The **Database Connection** window is displayed. In this window, set:
   - **Server Name**. This option defaults to the current machine.
   - **Database Name**. Select the Unified CCDM database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
   - **Authentication**. Select Windows Authentication.
3. Click **OK** to open ICE. The ICE Cluster Configuration tool starts by default.
4. From the Tool drop-down list, select **Replication Manager**. The Replication Manager opens in the Setup tab. The Setup tab has the following sections:
   - **Unified CCDM Database Server Properties** contains the publisher and subscriber Unified CCDM database details.
   - **Distributor Properties** contains the SQL Server Replication distributor properties.

   The default values shown in the Setup tab are derived from the values initially configured in the Cluster Configuration tool and will be suitable in most cases.
5. If required, modify the Unified CCDM Database Server Properties.
   - **Server Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.
   - **Catalog Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration. It may be changed, but if so, a valid database with the new name must already exist on the corresponding server.
6. If required, modify the distributor properties.
   - **Server Name**. The name of the subscriber server hosting the Unified CCDM database. This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.
   - **Catalog Name**. The name to be assigned to the distribution database. The recommended value is **distribution_portal**.
   - **Data Folder**. The folder path on the distributor server where the data file for the distribution database will be created.

Note
If you are setting up replication after performing an upgrade, be particularly careful with the Data Folder path, as it may be different from the value used in previous versions of Unified CCDM. Make sure you use the path that was specified when the database was set up.

- **Log Folder**. The folder path on the distributor server where the transaction log file for the distribution database will be created.
- **Distribution Share**. The distribution share folder where replication snapshot files will be generated.
- **Override Distributor Admin Password**. Select to override the auto-generated replication password which will be used to establish connectivity. The auto-generated password is 14 characters long, and will contain alpha-numeric characters (both upper and lower case) and a special character. If this does not meet the complexity requirements of the server then select this option and specify a password of your choice.

7. When you have set the required replication properties, click **Configure** to configure replication.
8. You may be prompted to save pending changes to the database before continuing. If so, click **Yes** to save pending changes and continue.
9. It may take several minutes to configure replication. Once replication has been configured, the Replication Manager automatically switches to the Monitor tab, which allows you to monitor the progress of the replication snapshot.

5.5.3 Monitor the Replication Snapshot

Note
The subscriber Database Server is not available for use until the replication snapshot has completed and all the data has been copied from the publisher database to the subscriber database.

To monitor the progress of the replication snapshot:

1. In the ICE Replication Manager, select the **Monitor** tab. The Monitor tab has the following panes:
   - **Publications** (top left) lists the publisher servers and the publications on each publisher that need to be shared with the subscribers.

- **Subscriptions and Agents** (top right) shows the subscriptions to a publication and the replication agents associated with a publication. This pane has two tabs, Subscriptions and Agents.
- **Subscriptions** shows the subscriptions to the selected publication. You can right-click on a subscription to start or stop the subscription.
- **Agents** shows the replication agents associated with the selected publication. You can right-click on a replication agent to start or stop the agent.
- **Sessions** (bottom left) shows all sessions for the selected publication and replication agent in the last 24 hours.
- **Actions** (bottom right) shows the activity for the selected session.

2. In the top left hand pane, select the first Unified CCDM database publication from the list of publications. If you have used the default database name, this will start with **[Portal]**.
3. Wait for the replication snapshot for this publication to complete.

   To check the replication status for a Unified CCDM database publication, in the bottom right hand pane of the Monitor tab, inspect the messages in the Action Message list. Once the replication snapshot is complete and replication is operational for a publication, you will see the following two messages:

   "Delivered snapshot from . . . "

   "No replicated transactions are available".

   After this, the second message is replaced with messages showing new replicated transactions as they are sent through the system, for example:

   "4 transaction(s) with 14 command(s) were delivered".
4. Repeat the two steps above for each of the remaining Unified CCDM database publications.
5. When replication is complete for all portal database publications, close the ICE tool.

The subscriber database can now be used to service requests. For more information about the Replication Manager see the *Administration Guide for Cisco Unified Contact Center Domain Manager*.

5.6 Unified CVP Media File Upload

5.6.1 About Unified CVP Media File Upload

Note
This configuration is only required where Unified CCDM Resource Management is deployed.

The Unified CVP media file upload allows you to provision WAV media files directly to the Unified CVP media server. This allows the associated WAV announcement for a Network VRU Script in Unified CCE to be replaced in near real-time. This solution requires your Unified CVP media server or servers to be hosted on Microsoft Windows 2000 Server, Microsoft Windows Server 2003 or Microsoft Windows Server 2008. The Unified CVP media servers and the web servers hosting Unified CCDM must belong to the same domain.

Unified CCDM writes media files to a domain share called **PortalMedia** on the domain controller. We recommend the use of Microsoft Distributed File System (DFS) to access the file system on the Unified CVP media servers. If you have multiple Unified CVP media servers, then Microsoft File Replication can be used to keep the announcement files in step across the servers.

5.6.2 Prepare the Configuration

Before configuring the Unified CVP Media File Upload solution for your network perform the following tasks:

1. Make a note of the Host Name and IP Addresses of the Unified CVP media server or servers.
2. Make a note of the User Name and Password of a user with administrator rights on the domain so that you can configure DFS and File Replication.
3. Ensure that Microsoft DFS, File Replication and Remote Procedure Call services are installed and running on the Unified CVP media servers and the domain controller.

5.6.3 Configure Unified CVP Media File Upload - Windows Server 2003

Follow the instructions in this section to configure Unified CVP media file upload if your domain controller is running Windows Server 2003.

5.6.3.1 Configure DFS for Unified CVP Media File Upload

This section describes how to create the shared folder to be used by each Unified CVP media server in the domain (Windows Server 2003 domain controllers only).

1. Login to the Domain Controller as a user with administrator rights.
2. Click **Start > Program Files > Administrative Tools > Distributed File System** to open the Distributed File System configuration utility.
3. Right-click on the Distributed File System node in the left of the screen and select **New Root** option to open the New Root Wizard.
4. Ensure that the option for **Domain Root** is selected in the **Root Type** window.
5. Follow the wizard by entering the default values. When you reach the **Host Server** window enter the Host Name of the Domain Controller.
6. For the Root Name field enter **PortalMedia** in the field provided.
7. For the **Folder to Share**, select the folder to contain the Unified CVP media files that are uploaded.

Note
This folder requires full access security permissions for the Domain Computers group. Configure this for both the shared permissions and the security credentials.

8. Click **Finish** to complete the action and add the root to the DFS utility.

5.6.3.2 Configure DFS Root Targets

For each media server that the Unified CVP Media File Upload will add files to, perform the following actions on the domain controller (Windows Server 2003 domain controllers only):

1. Right-click on the new root and select **New Root Target**.
2. Enter the server name for the Unified CVP media server.
3. For the **Folder to Share**, select the folder to contain the Unified CVP media files that are uploaded.

Note
This folder requires full access security permissions for the Domain Computers group. Configure this for both the shared permissions and the security credentials.

4. Click **Next** to create the Root Target.

5.6.3.3 Configure File Replication for Unified CVP Media File Upload

DFS shares must be setup on all the machines to which the media files should be copied, and file replication enabled among all of them.

The following steps will take you through the process of replicating files between the DFS shares (Windows Server 2003 domain controllers only). To enable this functionality you will need to ensure that the File Replication service is set to Automatic and is currently running.

To begin file replication:

1. Login to the Domain Controller as an administrative user.
2. Click **Start > Program Files > Administrative Tools > Distributed File System** to open the Distributed File System configuration utility.
3. Right-click Distributed File System node in the left hand panel and select **Show Root** option
4. Select **PortalMedia** node.
5. Right-click **PortalMedia** node located in the left hand panel of the Distributed File System window. Select **Configure Replication** option from the menu. The Configure Replication Wizard displays.
6. When prompted to select the initial master, select the share located on the domain controller.
7. Select **Full Mesh** topology for the replication set.
8. Click **Finish** to set up replication between the selected folders.

5.6.4 Configure Unified CVP Media File Upload - Windows Server 2008

Follow the instructions in this section to configure Unified CVP Media File Upload if your domain controller is running Windows Server 2008.

5.6.4.1 Create a Shared Namespace

To create a namespace on the domain controller to be used for replication (Windows Server 2008 domain controllers only):

1. Login to the Domain Controller as a user with administrator rights.
2. Click **Start > Program Files > Administrative Tools > Server Manager** to open the Server Manager utility.

3. In Server Manager, expand the **Roles** node, the **File Services** node, and the **DFS Management** node to see the Namespaces node. Right click on **Namespaces**, and select **New Namespace** to run the New Namespace Wizard.
4. In the Namespace Server window, enter the name of the primary Unified CCDM Database Server and click **Next**.
5. In the Namespace Name and Settings window, enter **PortalMedia** for the namespace name.

Note
The namespace name specified here must match the name shown by the ICE System Properties Manager tool, Media Upload group, Media Share property. The default is **PortalMedia**.

6. Click **Edit Settings**, review the shared folder permissions, and change them as required, if necessary. Click **OK**, then click **Next**.
7. In the Namespace Type window, select **Domain-based namespace** and click **Next**.
8. Review the namespace settings, and click **Create** to create the namespace you have specified. When the namespace has been created, click **Close**.

5.6.4.2 Configure Replication

To configure replication using the namespace you have just created (Windows Server 2008 domain controllers only):

1. On the domain controller, in the Server Manager utility, expand the **Roles** node, the **File Services** node, and the **DFS Management** node to see the Replication node. Right click on **Replication**, and select **New Replication Group** to run the New Replication Group Wizard.
2. In the Replication Group Type window, select **Multipurpose replication group**, and click **Next**.
3. In the Name and Domain window, enter a name for the replication group, for example, **sharePortalMedia**. Click **Next**.
4. In the Replication Group Members window, click **Add**, and in the Select Computers window, enter the name of one of the CVP media servers to be included in the replication group. Click **OK** to add the specified server to the replication group.
5. Repeat the step above to add each of the remaining CVP media servers to the replication group.
6. Click **Next**.

7. In the Topology Selection Window, select **Full mesh** and click **Next**.
8. In the Replication Group Schedule and Bandwidth window, select **Replicate continuously using the specified bandwidth** and click **Next**.
9. In the Primary Member window, choose one of the CVP media servers in the replication group to be the **Primary member**, and click **Next**.
10. In the Folders to Replicate window, click **Add**, then **Browse**. Select the folder on the primary server where the CVP media files are stored and click **OK**.
11. In the Local path on Other Members window, select one of the other CVP media servers in the replication group and click **Edit**.
12. In the Edit window, select **Enabled**, then **Browse**, and locate the folder on this server where the CVP media files are stored. Click **OK**.
13. Repeat the previous two steps for any other CVP media servers in the list of servers. Click **Next**.
14. Review the replication settings, and click **Create** to set up the replication you have specified. When the replication has been set up, click **Close**.

5.6.4.3 Share and Publish the Replicated Folder

To share and publish the replicated folder (Windows Server 2008 domain controllers only):

1. On the domain controller, in the Server Manager utility, expand the **Roles** node, the **File Services** node, and the **DFS Management** node to see the Replication node. Click on the replication group you created above, and select the **Replicated Folders** tab.
2. In the Publishing Method window, select **Share and Publish the Replicated Folder in a Namespace** and click **Next**.
3. In the Share Replicated Folders window, select one of the CVP media servers in the replication members section, and click **Edit**. Review the shared folder permissions, and change them as required, if necessary. Click **OK.**
4. Repeat the step above to set the folder permissions for each of the remaining CVP media servers in the replication group. Click **Next** when you have finished.
5. In the Namespace Path window, to set Parent folder in namespace, click **Browse**, select **\\<domain>\PortalMedia** from the list (this is the namespace you created above) and click **OK**.
6. In the Namespace Path window, enter the New folder name as **CVP**. Click **Next**.

7. Review the settings and click **Share** to publish the replicated folder.

5.6.4.4 Configure the Replicated Folder for Media File Upload

To configure Unified CCDM to use the replicated folder for CVP media file upload (Windows Server 2008 domain controllers only):

1. On the Unified CCDM Database Server, select **Start > All Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment.** The Database Connection dialog box is displayed.
2. Enter the database information for the primary Database Server and click **OK**.
3. In the ICE Cluster Configuration tool, in the **Tools** drop-down, select **System Properties Manager** and on the **Global** tab, navigate to the **Media Upload** group.
4. Change the Media Share property from the default value of **PortalMedia** to **PortalMedia\CVP.**
5. Select **File > Save** to save your changes. If you exit the tool without saving your changes you will be asked whether you want to save your changes when you exit the tool.
6. Close ICE.

5.6.5 Test the CVP Upload Configuration

You have now created and configured a DFS replicated location for Unified CCDM to use to upload media files.

The replicated location is of the form **<DomainName>\PortalMedia** and can be accessed by any machine in the domain. Files written to this location will be replicated to the specified folders on the servers in the replication group.

You can confirm that the replication for CVP media file upload is working by creating a file in **<DomainName>\PortalMedia** and ensuring that it is copied to all replication destinations.

6 Post-Installation Steps

6.1 About Post-Installation Steps

This chapter describes the remaining actions that must be taken to secure, configure and tune your installation. This chapter describes the following actions:

- configure SSL for the Unified CCDM web application and Web Services (required)
- configuring Single Sign-on (optional)
- configuring anti-virus options
- tuning your system for optimal performance
- performing the first log in and verifying the system

6.2 Configure SSL for Unified CCDM and Web Services

6.2.1 About Configuring SSL for Unified CCDM and Web Services

Follow the instructions below to configure SSL for the Unified CCDM web application and Web Services.

Note

These steps are mandatory and some features of the Unified CCDM web application will not work properly unless you do this.

These steps are also required if you are upgrading Unified CCDM, even if you have already configured SSL for a previous version.

To configure SSL for Unified CCDM you need to:

- obtain a digital certificate if you do not already have a suitable one (see section 6.2.2 "Obtain a Digital Certificate")
- configure SSL for the Unified CCDM web application (see section 6.2.3 "Configure SSL for Unified CCDM")
- grant network service rights to the certificate (see section 6.2.4 "Grant Network Service Rights to the Certificate")
- obtain the certificate thumbprint (see section 6.2.5 "Obtain the Certificate Thumbprint")

- configure Web Services to use the certificate (see section 6.2.6 "Configure Web Services to use the Certificate")
- test the certificate installation (see section 6.2.7 "Test the Certificate Installation").

6.2.2 Obtain a Digital Certificate

A digital certificate may be obtained in either of the following ways:

- purchased from an external certificate authority, for public use
- generated internally, for secure use within the issuing organization.

If you do not already have a suitable certificate, you can request or generate one as follows:

1. Open **Internet Information Services (IIS) Manager** and select the web server in the folder hierarchy.
2. Select the **Features View** tab, and in the **IIS** group, click on **Server Certificates**.
3. Create a digital certificate in one of the following ways:

Note
Take care to specify the Common Name exactly as specified below. The certificate will not work otherwise.

- To *request an external certificate*:
  - In the **Actions** pane, select **Create Certificate Request** to display the **Request Certificate** dialog box.
  - In the **Common Name** field, enter the fully qualified domain name of the web server. For example, if your web server is **WEBSERVER** and your domain name is **UCCDMDOM.LOCAL**, enter **WEBSERVER.UCCDMDOM.LOCAL**. If you have a load-balanced system, this must be the domain name of the load-balanced node, not the domain name of any of the individual servers.
  - Complete the other fields as appropriate, and click **Next**.
  - In the **Cryptographic Service Provider Properties** dialog box leave the default settings and click **Next**.
  - Specify a file name for the certificate, and then click **Finish**.

- When you receive the certificate from the certificate authority, repeat step 1. and step 2. above to show the Server Certificates and Action panes, and in the **Action** pane, select **Complete Certificate Request.**
- Enter the file name of the certificate, and a Friendly Name of your choice and click **OK**.

- To *generate an internal certificate*:
  - Select **Create Domain Certificate** in the **Actions** pane to display the **Distinguished Name Properties** dialog box.
  - In the **Common Name** field, enter the fully qualified domain name of the web server. For example, if your your web server is **WEBSERVER** and your domain name is **UCCDMDOM.LOCAL**, enter **WEBSERVER.UCCDMDOM.LOCAL**. If you have a load-balanced system, this must be the domain name of the load-balanced node, not the domain name of any of the individual servers.
  - Complete the other fields as appropriate, and click **Next**.
  - In the **Online Certification Authority** dialog box specify the **Online Authority** and **a Friendly Name**. Click **Finish.**

6.2.3 Configure SSL for Unified CCDM

Once you have a suitable digital certificate, configure SSL for Unified CCDM. On the App/Web Server:

1. Open **Internet Information Services (IIS) Manager**, expand the folder tree below the web server and select the web site that the Unified CCDM web application resides on.
2. In the Actions pane, select **Edit Site > Bindings** to display the Site Bindings dialog box.
3. If there no existing binding for https, click **Add** to display the Add Site Binding dialog box.
   - Set the **IP Address** to **All Unassigned**, and **Port** to **443**, unless your system has been set up differently. If you are unsure, contact your system administrator.
   - Set **SSL Certificate** to point to your certificate.
   - Click **OK**.

4. If there is an existing binding for https, select it and click **Edit** to display the Edit Site Binding dialog box, edit the settings to the values in step 3. above and click **OK**.
5. In the folder tree, select the **Portal** application.
6. Select the Features View tab, and click on **SSL Settings** in the **IIS** group.
7. Tick **Require SSL**, and leave the default **Ignore** for Client Settings.
8. In the Actions pane, click **Apply** to apply these settings.
9. Close IIS Manager.

6.2.4 Grant Network Service Rights to the Certificate

To grant network service rights to the certificate, on the App/Web Server:

1. In the Start menu, type **mmc** in the command box to open Microsoft Management Console (MMC).
2. Click **File > Add/Remove Snap-in**, click **Certificates**, then **Add**.
3. In the Certificates Snap-in dialog box, select **Computer Account** and click **Next**.
4. In the Select Computer dialog box, select **Local Computer** and click **Finish** to add the Certificates snap-in to MMC. Click **OK**.
5. In MMC, expand the Certificates node and the Personal node, then click **Certificates** to see the available certificates.
6. Right click on the certificate you want to use, select **All Tasks > Manage Private Keys**.
7. In the Permissions for Private Keys dialog box, click **Add**.
8. In the Select Users, Computers, Service or Groups dialog box, in the text box, type **NETWORK SERVICE**, then click **Check Names.** The name will be underlined if it has been entered correctly. Click **OK**.
9. In the Permissions for Private Keys dialog box, select the **NETWORK SERVICE** user, then in the Full Control row, select the check box in the **Allow** column. Click **OK**.

6.2.5 Obtain the Certificate Thumbprint

To obtain the certificate thumbprint, on the App/Web Server:

1. In MMC, expand the Certificates node and the Personal node to see the available certificates and select the certificate you want to use.
2. Double click on the certificate.

3. In the Certificate dialog box, select the **Details** tab, and click **Thumbprint**. The thumbprint for this certificate is displayed on the lower part of the screen as a text string.
4. Select the thumbprint text string, copy it and paste it into a text editor. Edit the string to remove all the spaces. For example, if the thumbprint text string you copied was:

   ```
   c3 34 9a 43 28 d3 a7 75 a9 93 eb 31 5c bf e0 62 51 6d b8 18
   ```

   you need to edit it to become:

   ```
   c3349a4328d3a775a993eb315cbfe062516db818
   ```

5. Save this thumbprint value as you will need it several times in the next step.

6.2.6 Configure Web Services to use the Certificate

To configure Web Services to use the certificate, on the App/Web Server:

1. Use Windows Services or the Service Manager in the ICE tool (see the *Administration Guide for Cisco Unified Contact Center Domain Manager*) to stop all Unified CCDM services.
2. Remove the existing localhost certificates for each of the Web Services by typing the following commands at the command prompt:
   - subscription manager

     ```
     netsh http delete sslcert ipport=0.0.0.0:8083
     ```

   - resource management

     ```
     netsh http delete sslcert ipport=0.0.0.0:8085
     ```

   - analytic data

     ```
     netsh http delete sslcert ipport=0.0.0.0:8087
     ```

3. Add the new certificates for each of the Web Services by typing the following commands at the command prompt, substituting the thumbprint value you obtained above instead of `<thumbprint>`:
   - subscription manager

     ```
     netsh http add sslcert ipport=0.0.0.0:8083
     certhash=<thumbprint>
     appid={16dde36c-787e-4dc7-bdc0-fd4ae0eb189a}
     ```

   - resource management

     ```
     netsh http add sslcert ipport=0.0.0.0:8085
     certhash=<thumbprint>
     appid={16dde36c-787e-4dc7-bdc0-fd4ae0eb189a}
     ```

- analytic data

```
netsh http add sslcert ipport=0.0.0.0:8087
certhash=<thumbprint>
appid={16dde36c-787e-4dc7-bdc0-fd4ae0eb189a}
```

For example, with the example thumbprint value from the section 6.2.5 "Obtain the Certificate Thumbprint", to update the subscription manager certificate, you would enter:

```
netsh http add sslcert ipport=0.0.0.0:8083
certhash= c3349a4328d3a775a993eb315cbfe062516db818
appid={16dde36c-787e-4dc7-bdc0-fd4ae0eb189a}
```

Note
Do not alter the `appid` value in the commands above.

6.2.7 Test the Certificate Installation

To test the certificate installation, in Internet Explorer, navigate to each of the locations below, where `<Server>` is the name of the App/Web Server.

Check that the page opens without a certificate warning, and that the address bar shows a green safe status.

`https://<Server>:8083/SubscriptionManager?wsdl`

`https://<Server>:8085/ResourceManagement?wsdl`

`https://<Server>:8086/HierarchyManagement?wsdl`

`https://<Server>:8087/AnalyticData?wsdl`

6.3 Configure Single Sign-On

6.3.1 About Single Sign-On

By default, Unified CCDM users need to login to Unified CCDM every time they connect. Unified CCDM can optionally be configured to use Single Sign-On (SSO), which links each Unified CCDM user account to their Windows user account and allows users to connect to Unified CCDM without logging in.

Note
Users cannot use SSO over a proxy connection.

Warning!
Setting up SSO will disable any existing Unified CCDM users which are not in domain login format. You will need to set up new Unified CCDM user accounts for all existing users.

6.3.2 Set Up Administrator Account

Warning!
It is vital that the new SSO administrator account is set up correctly since the existing Unified CCDM administrator account is disabled when SSO is configured.

1. Login to Unified CCDM as **administrator**.
2. In **User Manager**, create a user account to be the new administrator account. The login name should be of the form **<DOMAIN>\<your domain login>**, for example **ACMEDOM\jsmith**. The password should conform to the password security specified in System Settings, but will never be used.
3. Click **New User** and open **Groups** tab.
4. Click **Add to Group**.
5. Select the check box for the **Administrators** group.
6. Close and save.

6.3.3 Configure SSO Authentication

To configure SSO for Unified CCDM using ICE:

1. On the App/Web Server, select **Start > All Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment**.
2. In the **Database Connection** window specify the following:
   - **Server Name** This option defaults to the current machine.
   - **Database Name** Select the Unified CCDM database that was installed when setting up the Database Component. If you used the default value, this will be **Portal**.
   - **Authentication** Ensure this option is set to Windows Authentication.
3. In ICE, in the **Tools** drop-down, select **System Properties**. The System Properties tool is displayed.
4. In the **Global** properties tab, locate the **Login Authentication Configuration** group, **Login Authentication Mode** property.

5. Using the drop-down beside the property value, change the value from **Portal** to **Active Directory**.
6. Click **Save** to save the configuration change, then **Exit**.
7. On the App/Web Server, go to the location where Unified CCDM was installed (usually **C:\Program Files\Domain Manager**), right-click the **Web** folder and select **Properties**.
8. Select the **Security** tab, and ensure that all domain users have **Read** and **Read & Execute** permissions on this folder.
9. Click **Advanced** and ensure that **Include inheritable permissions from this object's parent** is selected. If this option is not selected, click **Change Permissions**, select it, and click **OK**.
10. Click **OK** to close the properties dialog.
11. From a command window, execute the **iisreset** command.

Users will now be able to access Unified CCDM directly from their domain account without needing to log in again.

Note

Depending on the way that Active Directory is configured in your installation, you may also need to change additional properties in the **Login Authentication Configuration** group in ICE System Properties. The default settings will be sufficient for most installations, but in some cases, you may need to change one or both of **Active Directory Binding Options** and **Active Directory Context Type** properties too.

For more information about the **Active Directory Binding Options** and **Active Directory Context Type** properties, see the *Administration Guide for Cisco Unified Contact Center Domain Manager*. For information about the values to choose for your Active Directory configuration, consult your Windows system administrator.

6.3.4 Manage Users with Single Sign-On

Once SSO has been set up, create a Unified CCDM login in the form `<DOMAIN>\<Windows domain login>` for Unified CCDM each user. Existing Unified CCDM user accounts will no longer be valid.

The first time a user accesses Unified CCDM using SSO a dialog box may appear requesting their Windows username and password. To sign in automatically in future, they will need to add the Unified CCDM website to the list of local intranet sites in their browser.

To add the Unified CCDM website to the list of local intranet sites in Internet Explorer:

1. Click **Tools** > **Internet Options**, and select the **Security** tab.
2. Select the **Local intranet** zone and click the **Sites** button.
3. Click **Advanced** to add the Unified CCDM site to IE's list of local intranet sites.
4. Enter the URL of the Unified CCDM website in **Add this website to the zone**, and click **Add**.
5. Click **OK** when prompted until you are returned to the browser window.

6.4 Configure Antivirus Options

If you have antivirus software on the Unified CCDM servers, we recommend that you exclude the following directories from the antivirus checks:

- The folders containing the database files (***.ldf**, ***.mdf** and ***.ndf**) on the Database Server. To locate these files, start **SQL Management Studio**, expand the **Databases** node, and select **Properties** for the database. If you selected the default database name at installation, the database will be **Portal**. In the Database Properties dialog box, select the **Files** page to see the folder and file names of the database files.
- The Importer folder on the Database Server. If you selected the default installation location, this will be **C:\Program Files\Domain Manager\Data Import Server\IMPORTER**.
- The Web folder and all subfolders on the App/Web Server. If you selected the default installation location, this will be **C:\Program Files\Domain Manager\Web**.

6.5 Performance Tuning Checklists

The following performance tuning steps will ensure optimal performance of Unified CCDM.

6.5.1 Web Server

Description	Done
Create a new page file, on a non-system drive, of minimum 1.5 x system memory and maximum 2 x system memory.	
Defragment the page file and registry hives using **http://www.sysinternals.com/Utilities/PageDefrag.html**.	

6.5.2 Database Server

Description	Done
Create a new page file, on a non-system drive, of minimum 1.5 x system memory and maximum 2 x system memory.	
Defragment page file and registry hives using **http://www.sysinternals.com/Utilities/PageDefrag.html**.	
Ensure the Portal database is set to **Simple Recovery Mode** on all systems.	

6.6 Final Post-Installation Actions

6.6.1 Restart the System

Reboot the servers after installation has finished, making sure that the Unified CCDM services start automatically on boot.

6.6.2 Log in to Unified CCDM

Unified CCDM can now be opened from **Start > All Programs > Domain Manager > Web > Domain Manager**. This will open a web page, which you can bookmark.

To login to a new system, use the username **administrator** and a blank password. You will be prompted to change this. If you are logging into an upgraded system, the administrator password will be the same as before.

Note
If you lose the administrator password, it cannot be reset except by another user with equal permissions. It is recommended that you note down the chosen password and keep it somewhere secure.

6.6.3 Verify the Installation

Once the system is installed and configured, you should run through the following checks to ensure that data is imported and the system running normally.

1. Log in to the Unified CCDM web application using the pre-configured **administrator** user and confirm that the Unified CCDM home page successfully displays.
2. Check that, on each Unified CCDM server, all the installed Unified CCDM services are started in **services.msc**.
3. Use the following SQL statement to confirm that resource data is being imported to the database:

```
Select count(*) from TB_DIM_AGENT
```

This query should return a value of at least 3.

7 Upgrading From a Previous Version

7.1 About the Upgrade Procedure

The upgrade procedure for Unified CCDM depends on your deployment model, and your requirements for the upgrade. For example, a upgrading a single server system is simpler than upgrading a resilient two-tier system where down-time must be minimized. The upgrade procedure may also depend on the version of Unified CCDM that you are upgrading from. This chapter describes several upgrade methods. Read this chapter, then choose the method that best suits your system configuration and upgrade requirements.

This table lists the different upgrade procedures described in this document and the scenarios where they can be used.

Upgrade Procedure	Upgrade Requirement				
	Single-sided system	Dual-sided system	Minimal downtime	Simple process	Dual-sided with different s/w versions
Single Sided Upgrade (see Chapter 8 "Single-Sided Upgrade")	✓		✓	✓	
Total Outage Upgrade (see Chapter 9 "Total Outage Upgrade")		✓		✓	
Split Side Upgrade (see Chapter 10 "Split Side Upgrade")		✓	✓		✓

7.2 About Upgrading Dual-Sided Systems

Unified CCDM employs a distributed architecture for dual-sided systems.

When upgrading the platform the design and architecture must be considered to ensure the minimal amount of down-time is achieved and no data loss is incurred.

Resilience is achieved by the use of a second side of the system containing the same components as the primary side.

SQL Server replication is used to replicate data from Side A to Side B and Side B to Side A.

Failover information for the individual Unified CCDM components is stored in the databases on Side A and B. This information is also replicated using SQL Server replication. This means that both sides have knowledge of the primary and secondary server configuration made through the Unified CCDM Integrated Configuration Management tool, even when replication has been removed.

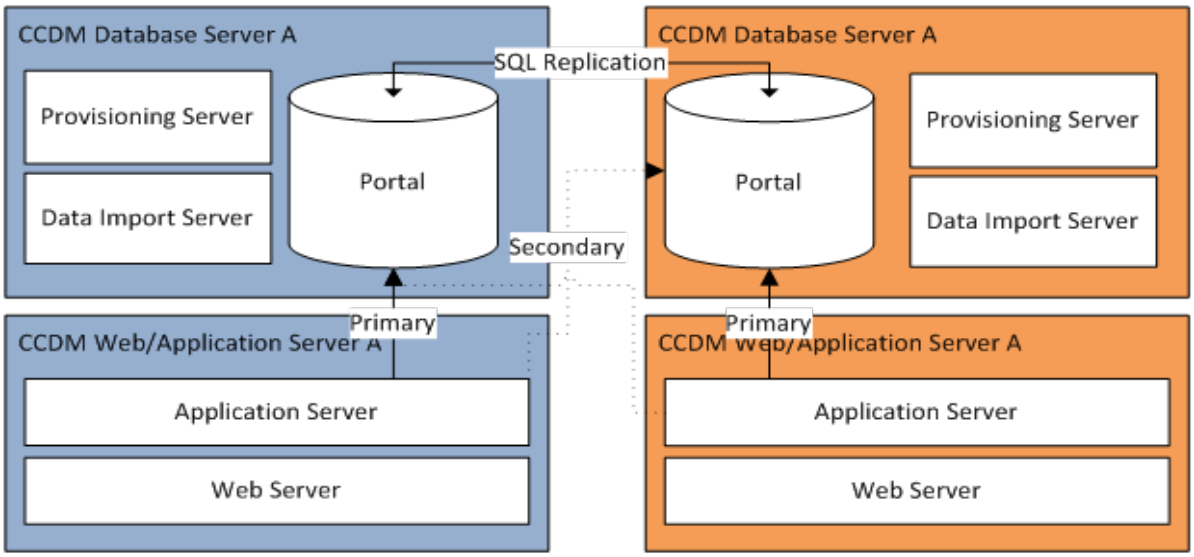

Figure 7.1 Replication and Failover Connections

When a replicated system is upgraded one side at a time, it is possible for the individual components of Unified CCDM to fail-over to the other non-upgraded side. This will result in data inconsistencies as some data is entered to Side A and some to Side B with no replication running to synchronize the two sides.

There are two ways to upgrade dual-sided systems:

- If it is acceptable for the system to be completely unavailable whilst the upgrade is performed, then use the Total Outage Upgrade method. This is the quicker upgrade method.
- If high-availability is required, then use the Split-Sided Upgrade method. This method maximizes the system up time during the upgrade but adds additional complexity.

7.3 Validating an Upgrade

After you have upgraded your installation of Unified CCDM, check that the system is functional following the upgrade with the following tests.

Check	Success Criteria
Unified CCE Provisioning Tests	
Log in to the web application on Side A and create a new Skill Group. This tests provisioning from the Side A App/Web Server. Run this test against each configured Unified CCE instance.	The Skill Group should be successfully created, and visible on Side A, and, if applicable, Side B.
Log in to the web application on Side A and create a new Agent This tests provisioning from the Side A App/Web Server. Run this test against each configured Unified CCE instance.	The Agent should be successfully created and visible on Side A, and, if applicable, Side B.
Create a new Skill Group on the AW using the Cisco Skill Group Explorer tool. Wait a few minutes and check that the Skill Group has been imported into Unified CCDM.	The Skill Group should be visible on Side A, and, if applicable, on Side B.
CUCM Provisioning Tests	
Log in to the web application on Side A and create a new IP Phone. This tests Unified CM provisioning from the Side A App/Web Server.	The IP Phone should be successfully created, and be visible on Side A, and, if applicable, on Side B.
Replication Tests (dual-sided installations only)	
Log in to the web application on Side B and create a new Skill Group. This tests Unified CCE provisioning from the Side B App/Web Server. Run this test against each configured Unified CCE instance.	The Skill Group should be successfully created, and visible on Side A.
Create a new Skill Group on the AW using the Cisco Skill Group Explorer tool. Wait a few minutes and check that the Skill Group has been imported into Unified CCDM.	The Skill Group should be visible on Side A and Side B.
Log in to the web application on Side B and create a new IP Phone. This tests Unified CM provisioning from the Side B App/Web Server.	The IP Phone should be visible on Side A and Side B.

8 Single-Sided Upgrade

8.1 About a Single-Sided Upgrade

This chapter describes the steps involved to upgrade a single-sided deployment. The description assumes that you have a two tier deployment (separate database and app/web servers).

Note
Before starting the upgrade please ensure you have the original cryptographic passphrase from the original Unified CCDM installation as you will need it during the upgrade.

8.2 Checklist for Single-Sided Upgrades

Step	Complete
Prepare the Unified CCDM servers	
Stop the Unified CCDM Services	
Backup the Unified CCDM Portal databases	
Uninstall Existing Unified CCDM Software	
Uninstall the Database Server Components	
Uninstall the App/Web Server Components	
Install the new Unified CCDM Components and upgrade Portal database	
Install the Unified CCDM Database Installer	
Upgrade the Unified CCDM Portal database	
Install the Unified CCDM App/Web Server	
Configure the Unified CCE Config Web Service	
Restart and Validate	
Restart the Unified CCDM Services	
Validate the upgrade	

8.3 Prepare the Unified CCDM Servers

8.3.1 Stop the Unified CCDM Services

Before starting the upgrade, stop the Unified CCDM services on all servers.

Data Import Server Service

To stop the Unified CCDM: Data Import Server service, on the Database Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the UCCDM**: Data Import Server** service in the list of services.
4. Select **Stop**.
5. Close the Services window.

Partition Table Manager Service

To stop the Unified CCDM: Partition Table Manager service, on the Database Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the UCCDM**: Partitioning Table Manager** service from the list of services.
4. Select **Stop**.
5. Close the Services window

Provisioning Server Service

To stop the Unified CCDM: Provisioning Server service, on the Database Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the UCCDM**: Provisioning Server** service from the list of services.
4. Select **Stop**.
5. Close the Services window.

System Monitoring Services and Other Services

To stop the remaining Unified CCDM services, on the App/Web Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the Unified CCDM**: System Monitoring Services** service from the list of services.
4. Select **Stop**.
5. At the message: “When UCCDM: System Monitoring Services stops, these other services will also stop. Do you want to stop these services?”, click **Yes**.
6. Close the Services window.

8.3.2 Back up the Unified CCDM Portal Database

Back up the Unified CCDM Portal database so that you can restore it in the event of a failure.

On the Database Server:

1. Click **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**
2. Connect to the Database Engine using Windows Authentication.
3. Navigate to the Portal database.
4. Right-click **Portal** and select **Tasks > Back Up**.
5. Amend the Destination as appropriate using the Remove and Add features
6. Click **OK**.
7. Close the SQL Server Management Studio window.

8.4 Uninstall Existing Unified CCDM Software

8.4.1 Uninstall the Database Server Components

On the Database Server:

1. Click **Start > Control Panel > Uninstall a program**.
2. In the Programs and Features window, select **Domain Manager: Database Components.**
3. Click **Uninstall** then **Yes** to confirm.The Setup Status window displays, showing the progress of the uninstallation.
4. When the uninstallation is complete, close the Programs and Features window.

8.4.2 Uninstall the App/Web Server Components

On the App/Web Server:

1. Click **Start > Control Panel > Uninstall a program**.
2. Select **Domain Manager: Application Server Components.**
3. Click **Uninstall** then **Yes** to confirm.The Setup Status window displays, showing the progress of the uninstallation.
4. When the uninstall is complete, the App/Web Server will reboot automatically.

8.5 Install New Unified CCDM Components and Upgrade Portal Database

8.5.1 Install the Database Installer

This process does not upgrade the database directly. It just installs the Database Installer which is then used to upgrade the database.

On the Database Server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see section 4.2.1 "About the Unified CCDM Installer").
2. Select **Database Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.
3. When all checks have passed, click **Install** to begin the Database Server Installation. The Setup window displays.
4. Click **Next** to go through each window in turn. You will need to enter the following details:
5. In the License Agreement window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.
6. In the Cryptography Configuration window:
   - **Passphrase.** Enter the cryptographic passphrase you created during installation of the Database Server component when you first installed Unified CCDM. If you continue installation with a new passphrase, you will be unable to access your existing data

- **Confirm Passphrase.** You will not be able to continue until the contents of this field are identical to the passphrase entered above.

Warning!
You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you do not know the cryptographic passphrase, **stop the installation immediately** and contact your vendor. If you continue the installation with a new passphrase you will be unable to access your existing data.

7. In the Configure Database window:
   - **Database Name**. Enter the name of the database catalog for Unified CCDM. By default this is **Portal**.
   - **Connect Using**. Select the login credentials you want to use:
     - **Windows Authentication Credentials of Application**. This is the recommended option.
     - **SQL Server Authentication using the login and password below**. This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your SQL Server Login Name and Password in the fields provided.
   - **Click Next.**
8. In the Destination Folder window, you can click **Change** to change the location where the Database components are installed. It is not necessary to install all Unified CCDM components in the same location.
9. Click **Install** to install the Database Installer.

Note
During the Database Install Tool Installation, the J2SE pre-requisite will be automatically installed if it is not already present. You may see a Security Alert dialog box stating that 'Revocation Information for the security certificate for this site is not available'. If so, click **Yes** to continue.

10. To install or upgrade your database immediately after installing the Database Installer, select the **Launch Database Management Utility** check box at the end of the installation before clicking Finish.
11. Click **Finish**.

8.5.2 Upgrade the Portal Database

Once the Database Installer is installed, it can be used to upgrade the database.

On the Database Server:

1. If you selected the Launch Database Management Utility check box when you installed the Database Installer, the Database Installer launches automatically after it has been installed. Otherwise, launch the Database Installer manually from **Start > All Programs >** Domain Manager **> Database > Database Installer**. The Database Installer is a wizard which guides you through the steps to upgrade the database.
2. Click **Next** to begin the upgrade process.
3. In the Database Setup Window choose **Upgrade an Existing Database**. Click **Next** to continue.
4. In the SQL Server Connection Details window, take the following actions:
   - **Server Name**. Select the Microsoft SQL Server where the Unified CCDM database is located. In this case this is the machine running the application, and so it must be left as the default (local).
   - **Database Name**. Enter or select the name of the database catalog that was originally used for the Unified CCDM database.
   - **Connect Using**. Select the login credentials you want to use:
     - The **Windows account information you use to log in to your computer**. This is the recommended option.
     - The **Microsoft SQL Server login information assigned by the system administrator**. Only select this option if you are using a database catalog on a different domain. For this option you must enter your Login Name and Password in the fields provided.
   - **Test Connection**. Click to make sure the connection to the Microsoft SQL Server is established. If you see the message 'Connection succeeded but database does not exist' then you must rectify this problem before continuing. Check that the database catalog name and security credentials are correct.
   - When the database connection details have been tested and the connection is successful, click **Next**.
5. Click **Next** to perform the upgrade. The upgrade may take several minutes.
6. When the Portal database upgrade is complete, click **Close** to close the Database Installer.

8.5.3 Install the App/Web Server

On the App/Web Server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see section 4.2.1 "About the Unified CCDM Installer").
2. Select **App/Web Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.
3. When all checks have passed, click **Install** to begin the App/Web Server installation. The **Domain Manager: Application Server Component** window displays.
4. Click **Next** to go through each window in turn. You will need to enter the following details:
5. If the Domain Manager: Application Server Components Dialog is displayed, click **Install** to install the additional required components.
6. If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.5 Framework is complete, restart the server to continue the installation of the App/Web Server.
7. In the **License Agreement** window:
   - **I accept the terms in the license agreement**. You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.
8. In the **Cryptography Configuration** window:
   - **Passphrase**. Enter the cryptographic passphrase you created during installation of the Database Server component.
   - **Confirm Passphrase**. You will not be able to continue until the contents of this field are identical to the passphrase entered above.
   - Click **Next** to continue.

Warning!
You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you do not know the cryptographic passphrase, **stop the installation immediately** and contact your vendor. If you continue the installation with a new passphrase you will be unable to access your existing data.

9. In the **Destination Folder** window, you can click **Change** to change the location that the App/Web Server components are installed to. Click **Next** to continue.

10. In the **Configure Database** window:
    - **SQL Server Name**. Enter the host name or IP Address of the server hosting the Unified CCDM database. The default name of **localhost** is only valid if you are installing this component on the Database Server. Otherwise, specify the name of the Database Server. For a dual-sided deployment enter the name of the Side A Database server when installing the Side A components and enter the name of the Side B Database Server when installing the Side B components.
    - **Catalog Name**. Enter or select the database catalog name you specified when installing the Database Server component. If you used the default value, this will be **Portal**.
    - **Connect Using**. Select the login credentials you want to use:
        - **Windows authentication.** This is the recommended option.
        - **SQL Server authentication.** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter a SQL Server Login Name and Password in the fields provided.
    - Click **Next** to continue.
11. Click **Install**.
12. When the installation has completed, click **Finish**.

Note
The machine will restart once the installation is complete.

8.5.4 Configure the Unified CCE Config Web Service

On the Database Server, the Unified CCE Config Web Service must be configured for each connected Unified CCE Server.

To configure the Unified CCE Config Web Service, on the Database Server:

1. Go to **Start > All Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment**.
2. The **Database Connection** window is displayed. In this window, set:
    - **Server Name**. This option defaults to the current machine.
    - **Database Name**. Select the Unified CCDM database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
    - **Authentication**. Select Windows Authentication.

3. Click **OK** to open Unified CCDM Integrated Configuration Environment.
4. Select the **Setup** tab and click **Configure Cisco Unified CCE Servers** to start the wizard. Click **Next** to go through each window in turn.
5. In the Select Task dialog box select **Modify an existing instance**.
6. Select the Unified CCE instance you want to modify and click **Next**.
7. Complete the dialog boxes as follows:
   - In the Configure Primary Unified Config Web Service dialog box, enter the following details
     - **URL**. This is the auto-generated URL of the primary Unified Config Web Service on the Unified CCE.
     - **User Name**. This is a username with appropriate access to the Unified CCE that the web service is running on. This user must be in the domain security group **<Server>_<UCCE-Instance>_ Config**, where <Server> is the name of the server running Unified CCE and <UCCE-Instance> is the name of the Unified CCE Instance on this server.
     - **Password**. This is the password for the user.
   - In the Configure Primary ConAPI RMI Ports dialog box enter the following ConAPI details:
     - **Local Registry Port**. This is the port on the Unified CCE for the Unified CCDM Provisioning service to connect to. This will usually be 2099.
     - **Remote Registry Port**. This is the port on the Unified CCDM Database Server for the Unified CCE to connect to. This will usually be 2099.
     - **Local Port**. This is selected as the designated port for live provisioning traffic between the Unified CCE and Unified CCDM servers. It must be uniquely assigned for each Unified CCE and any firewalls between the CICM and Unified CCDM server must be configured to allow both-way traffic on this port.
   - In the Configure ConAPI Application Instance dialog box enter the following details:
     - **Application Name.** The name of the application to be used for provisioning Unified CCE from Unified CCDM. Specify the name of the application you configured in section 5.3.2 "Set Up ConAPI".

- **Application Key.** Use the password for the application you specified above.

- In the Multi Media Support dialog box, if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance to provide support for non-voice interactions, select **Yes**. The default is No.
- In the Purge On Delete dialog box, if you want to purge items from Unified CCE automatically when they are deleted from Unified CCDM, select **Yes**. The default is Yes.
- In the Supervisor Active Directory Integration dialog box, if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors, select **Yes**. The default is No. If you select Yes, you will be prompted to provide Active Directory information so that Windows user accounts can be listed.

8. The Summary dialog box summarizes the details of the Unified CCE being configured and the settings you have chosen. Check the details, and if you are satisfied, click **Next**.
9. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.
10. For each remaining Unified CCE Server, click **Configure Cisco Unified CCE Servers**, and repeat the steps above.
11. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu.

8.6 Restart and Validate

8.6.1 Restart the Unified CCDM Services

Following an upgrade it is good practice to restart all Unified CCDM services.

Repeat the following steps on each Unified CCDM Database Server and each and Unified CCDM App/Web Server:

1. Click **Start > Run.**
2. Enter **Services.msc** and then click **OK**.
3. For each Unified CCDM service listed:
   - if the selected service is in the Started state, right click the service name and click **Restart**
   - if the selected service is not started, right-click the service name and click **Start**.

Note
After starting the System Monitoring Service and Application Service on the App/Web Server, you will need to wait a few minutes before logging in to allow the services to load completely.

8.6.2 Validate the Upgrade

Check that the system is functional following the upgrade using the validation tests in section 7.3 "Validating an Upgrade".

9 Total Outage Upgrade

9.1 About a Total Outage Upgrade

This chapter describes the steps involved to upgrade a dual-sided deployment, where all servers will be taken down and upgraded at once. The description assumes that you have a two tier deployment (separate database and app/web servers).

Note
Before starting the upgrade please ensure you have the original cryptographic passphrase from the original Unified CCDM installation as you will need it during the upgrade.

9.2 Checklist for Total Outage Upgrades

Step	Complete
Prepare the Unified CCDM servers	
Stop the Unified CCDM Services	
Remove database replication	
Backup the Side A and Side B Portal databases	
Uninstall Existing Unified CCDM Software	
Uninstall the Database Server Components from both Database Servers.	
Uninstall the App/Web Server Components from both App/Web Servers	
Install the new Unified CCDM Components and upgrade the Portal database	
Install the new Unified CCDM Database Installer on both Database Servers	
Upgrade the Unified CCDM Portal database on both Database Servers	
Install the Unified CCDM App/Web Servers on both App/Web Servers.	
Configure the Unified CCE Config Web Service	

Step	Complete
Restore Replication	
Restore replication between the Side A and Side B databases.	
Monitor the Replication Snapshot	
Confirm the replication snapshot has completed	
Restart and Validate	
Restart the Unified CCDM Services	
Validate the upgrade	

9.3 Prepare Unified CCDM Servers

9.3.1 Stop the Unified CCDM Services

Before starting the upgrade stop the Unified CCDM services on all servers.

Stop the following services on the Side A servers.

Data Import Server Service

To stop the Unified CCDM: Data Import Server service, on the Database Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the UCCDM**: Data Import Server** service in the list of services.
4. Select **Stop**.
5. Close the Services window.

Partition Table Manager Service

To stop the Unified CCDM: Partition Table Manager service, on the Database Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the UCCDM**: Partitioning Table Manager** service from the list of services.
4. Select **Stop**.

5. Close the Services window

Provisioning Server Service

To stop the Unified CCDM: Provisioning Server service, on the Database Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the UCCDM**: Provisioning Server** service from the list of services.
4. Select **Stop**.
5. Close the Services window.

System Monitoring Services and Other Services

To stop the remaining Unified CCDM services, on the App/Web Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the Unified CCDM**: System Monitoring Services** service from the list of services.
4. Select **Stop**.
5. At the message: "When UCCDM: System Monitoring Services stops, these other services will also stop. Do you want to stop these services?", click **Yes**.
6. Close the Services window.

Repeat the steps above on the Side B servers.

9.3.2 Remove Portal Database Replication

Before the upgrade can proceed, portal database replication must be removed.

To remove portal database replication:

1. Ensure you are logged in to the Side A Database Server as a domain level user with administrative rights over both Database Servers.
2. In your Windows desktop, click **Start > Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment**.
3. The **Database Connection** window is displayed. In this window, set:
   - **Server Name** This option defaults to the current machine.
   - **Database Name** Select the Unified CCDM database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

- **Authentication** Select Windows Authentication.

4. Click **OK** to open Unified CCDM Integrated Configuration Environment.
5. The Cluster Configuration tool is open by default. From the Tool drop-down list select **Replication Manager**.
6. Click the **Setup** tab to see the replication setup details.
7. Click **Disable** to remove replication from the Unified CCDM database. When prompted, click **Yes** to proceed with replication removal.
8. Replication removal may take several minutes. Wait for the 'Replication Removed' message to display in the Output Window and then exit ICE.

9.3.3 Back up the Portal Databases

Back up the Unified CCDM Portal databases so that you can restore them in the event of a failure.

On the Side A Database Server:

1. Click **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**
2. Connect to the Database Engine using Windows Authentication.
3. Navigate to the Portal database.
4. Right-click **Portal** and select **Tasks > Back Up**.
5. Amend the Destination as appropriate using the Remove and Add features
6. Click **OK**.
7. Close the SQL Server Management Studio window.

Repeat this process for the Unified CCDM Portal database on the Side B Database Server.

9.4 Uninstall Existing Unified CCDM Software

9.4.1 Uninstall the Database Server Components

On the Side A Database Server:

1. Click **Start > Control Panel > Uninstall a program**.
2. In the Programs and Features window, select **Domain Manager: Database Components.**
3. Click **Uninstall** then **Yes** to confirm.The Setup Status window displays, showing the progress of the uninstallation.

4. When the uninstallation is complete, close the Programs and Features window.

Repeat this process on the Side B Database Server.

9.4.2 Uninstall the App/Web Server Components

On the Side A App/Web Server:

1. Click **Start > Control Panel > Uninstall a program**.
2. Select **Domain Manager: Application Server Components.**
3. Click **Uninstall** then **Yes** to confirm.The Setup Status window displays, showing the progress of the uninstallation.
4. When the uninstall is complete, the App/Web Server will reboot automatically.

Repeat this process on the Side B App/Web Server.

9.5 Install New Components and Upgrade Portal Database

9.5.1 Install the Database Installer

This process does not upgrade the database directly. It just installs the Database Installer which is then used to upgrade the database.

On the Side A Database Server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see section 4.2.1 "About the Unified CCDM Installer").
2. Select **Database Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.
3. When all checks have passed, click **Install** to begin the Database Server Installation. The Setup window displays.
4. Click **Next** to go through each window in turn. You will need to enter the following details:
5. In the License Agreement window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.
6. In the Cryptography Configuration window:

- **Passphrase.** Enter the cryptographic passphrase you created during installation of the Database Server component when you first installed Unified CCDM. If you continue installation with a new passphrase, you will be unable to access your existing data
- **Confirm Passphrase.** You will not be able to continue until the contents of this field are identical to the passphrase entered above.

Warning!
You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you do not know the cryptographic passphrase, **stop the installation immediately** and contact your vendor. If you continue the installation with a new passphrase you will be unable to access your existing data.

7. In the Configure Database window:
   - **Database Name**. Enter the name of the database catalog for Unified CCDM. By default this is **Portal**.
   - **Connect Using**. Select the login credentials you want to use:
     - **Windows Authentication Credentials of Application**. This is the recommended option.
     - **SQL Server Authentication using the login and password below**. This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your SQL Server Login Name and Password in the fields provided.
   - **Click Next.**
8. In the Destination Folder window, you can click **Change** to change the location where the Database components are installed. It is not necessary to install all Unified CCDM components in the same location.
9. Click **Install** to install the Database Installer.

Note
During the Database Install Tool Installation, the J2SE pre-requisite will be automatically installed if it is not already present. You may see a Security Alert dialog box stating that ‘Revocation Information for the security certificate for this site is not available'. If so, click **Yes** to continue.

10. To install or upgrade your database immediately after installing the Database Installer, select the **Launch Database Management Utility** check box at the end of the installation before clicking Finish.

11. Click **Finish**.

Repeat the steps above to install the Database Installer process on the Side B Database Server.

9.5.2 Upgrade the Portal Database

Once the Database Installer is installed, it can be used to upgrade the database.

On the Side A Database Server:

1. If you selected the Launch Database Management Utility check box when you installed the Database Installer, the Database Installer launches automatically after it has been installed. Otherwise, launch the Database Installer manually from **Start > All Programs >** Domain Manager **> Database > Database Installer**. The Database Installer is a wizard which guides you through the steps to upgrade the database.
2. Click **Next** to begin the upgrade process.
3. In the Database Setup Window choose **Upgrade an Existing Database**. Click **Next** to continue.
4. In the SQL Server Connection Details window, take the following actions:
   - **Server Name**. Select the Microsoft SQL Server where the Unified CCDM database is located. In this case this is the machine running the application, and so it must be left as the default (local).
   - **Database Name**. Enter or select the name of the database catalog that was originally used for the Unified CCDM database.
   - **Connect Using**. Select the login credentials you want to use:
     - The **Windows account information you use to log in to your computer**. This is the recommended option.
     - The **Microsoft SQL Server login information assigned by the system administrator**. Only select this option if you are using a database catalog on a different domain. For this option you must enter your Login Name and Password in the fields provided.
   - **Test Connection**. Click to make sure the connection to the Microsoft SQL Server is established. If you see the message 'Connection succeeded but database does not exist' then you must rectify this problem before continuing. Check that the database catalog name and security credentials are correct.
   - When the database connection details have been tested and the connection is successful, click **Next**.
5. Click **Next** to perform the upgrade. The upgrade may take several minutes.

6. When the Portal database upgrade is complete, click **Close** to close the Database Installer.

Repeat the steps above to upgrade the portal database on the Side B Database Server.

9.5.3 Install the App/Web Server

Install the new App/Web Server components on the Side A and Side B App/Web Servers.

On the Side A Web Server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see section 4.2.1 "About the Unified CCDM Installer").
2. Select **App/Web Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.
3. When all checks have passed, click **Install** to begin the App/Web Server installation. The **Domain Manager: Application Server Component** window displays.
4. Click **Next** to go through each window in turn. You will need to enter the following details:
5. If the Domain Manager: Application Server Components Dialog is displayed, click **Install** to install the additional required components.
6. If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.5 Framework is complete, restart the server to continue the installation of the App/Web Server.
7. In the **License Agreement** window:
   - **I accept the terms in the license agreement**. You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.
8. In the **Cryptography Configuration** window:
   - **Passphrase**. Enter the cryptographic passphrase you created during installation of the Database Server component.
   - **Confirm Passphrase**. You will not be able to continue until the contents of this field are identical to the passphrase entered above.
   - Click **Next** to continue.

Warning!
You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you do not know the cryptographic passphrase, **stop the installation immediately** and contact your vendor. If you continue the installation with a new passphrase you will be unable to access your existing data.

9. In the **Destination Folder** window, you can click **Change** to change the location that the App/Web Server components are installed to. Click **Next** to continue.
10. In the **Configure Database** window:
    - **SQL Server Name**. Enter the host name or IP Address of the server hosting the Unified CCDM database. The default name of **localhost** is only valid if you are installing this component on the Database Server. Otherwise, specify the name of the Database Server. For a dual-sided deployment enter the name of the Side A Database server when installing the Side A components and enter the name of the Side B Database Server when installing the Side B components.
    - **Catalog Name**. Enter or select the database catalog name you specified when installing the Database Server component. If you used the default value, this will be **Portal**.
    - **Connect Using**. Select the login credentials you want to use:
        - **Windows authentication.** This is the recommended option.
        - **SQL Server authentication.** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter a SQL Server Login Name and Password in the fields provided.
    - Click **Next** to continue.
11. Click **Install**.
12. When the installation has completed, click **Finish**.

Note
The machine will restart once the installation is complete.

Repeat the installation steps on the Side B Web Server.

9.5.4 Configure the Unified CCE Config Web Service

On the Side A Database Server, the Unified CCE Config Web Service must be configured for each connected Unified CCE Server.

To configure the Unified CCE Config Web Service, on the Side A Database Server:

1. Go to **Start > All Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment**.
2. The **Database Connection** window is displayed. In this window, set:
   - **Server Name**. This option defaults to the current machine.
   - **Database Name**. Select the Unified CCDM database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
   - **Authentication**. Select Windows Authentication.
3. Click **OK** to open Unified CCDM Integrated Configuration Environment.
4. Select the **Setup** tab and click **Configure Cisco Unified CCE Servers** to start the wizard. Click **Next** to go through each window in turn.
5. In the Select Task dialog box select **Modify an existing instance**.
6. Select the Unified CCE instance you want to modify and click **Next**.
7. Complete the dialog boxes as follows:
   - In the Configure Primary Unified Config Web Service dialog box, enter the following details
     - **URL**. This is the auto-generated URL of the primary Unified Config Web Service on the Unified CCE.
     - **User Name**. This is a username with appropriate access to the Unified CCE that the web service is running on. This user must be in the domain security group **<Server>_<UCCE-Instance>_ Config**, where <Server> is the name of the server running Unified CCE and <UCCE-Instance> is the name of the Unified CCE Instance on this server.
     - **Password**. This is the password for the user.
   - In the Configure Primary ConAPI RMI Ports dialog box enter the following ConAPI details:
     - **Local Registry Port**. This is the port on the Unified CCE for the Unified CCDM Provisioning service to connect to. This will usually be 2099.
     - **Remote Registry Port**. This is the port on the Unified CCDM Database Server for the Unified CCE to connect to. This will usually be 2099.

- **Local Port**. This is selected as the designated port for live provisioning traffic between the Unified CCE and Unified CCDM servers. It must be uniquely assigned for each Unified CCE and any firewalls between the CICM and Unified CCDM server must be configured to allow both-way traffic on this port.

- In the Configure ConAPI Application Instance dialog box enter the following details:
  - **Application Name.** The name of the application to be used for provisioning Unified CCE from Unified CCDM. Specify the name of the application you configured in section 5.3.2 "Set Up ConAPI".
  - **Application Key.** Use the password for the application you specified above.
- In the Multi Media Support dialog box, if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance to provide support for non-voice interactions, select **Yes**. The default is No.
- In the Purge On Delete dialog box, if you want to purge items from Unified CCE automatically when they are deleted from Unified CCDM, select **Yes**. The default is Yes.
- In the Supervisor Active Directory Integration dialog box, if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors, select **Yes**. The default is No. If you select Yes, you will be prompted to provide Active Directory information so that Windows user accounts can be listed.

8. The Summary dialog box summarizes the details of the Unified CCE being configured and the settings you have chosen. Check the details, and if you are satisfied, click **Next**.
9. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.
10. For each remaining Unified CCE Server, click **Configure Cisco Unified CCE Servers**, and repeat the steps above.
11. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu.

9.6 Restore Replication

9.6.1 Restore Unified CCDM Database Replication

For a dual-sided deployment, you must reinstate replication between the Side A and Side B portal databases. Replication between the databases is set up and monitored using the Replication Manager application which is available in the Unified CCDM Integrated Configuration Environment (ICE) tool.

Note

The user running Replication Manager must have administrator permissions in both Windows and SQL Server, for both the publisher and the subscriber Database Servers.

Usually, the publisher will be the Side A Database Server, but occasionally, it may be necessary to configure the Side B Database Server as the publisher.

To configure replication, on the publisher Database Server:

1. Go to **Start > All Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment**.
2. The **Database Connection** window is displayed. In this window, set:
   - **Server Name**. This option defaults to the current machine.
   - **Database Name**. Select the Unified CCDM database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
   - **Authentication**. Select Windows Authentication.
3. Click **OK** to open ICE. The ICE Cluster Configuration tool starts by default.
4. From the Tool drop-down list, select **Replication Manager**. The Replication Manager opens in the Setup tab. The Setup tab has the following sections:
   - **Unified CCDM Database Server Properties** contains the publisher and subscriber Unified CCDM database details.
   - **Distributor Properties** contains the SQL Server Replication distributor properties.

   The default values shown in the Setup tab are derived from the values initially configured in the Cluster Configuration tool and will be suitable in most cases.
5. If required, modify the Unified CCDM Database Server Properties.

- **Server Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.
- **Catalog Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration. It may be changed, but if so, a valid database with the new name must already exist on the corresponding server.

6. If required, modify the distributor properties.
   - **Server Name**. The name of the subscriber server hosting the Unified CCDM database. This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.
   - **Catalog Name**. The name to be assigned to the distribution database. The recommended value is **distribution_portal**.
   - **Data Folder**. The folder path on the distributor server where the data file for the distribution database will be created.

Note
If you are setting up replication after performing an upgrade, be particularly careful with the Data Folder path, as it may be different from the value used in previous versions of Unified CCDM. Make sure you use the path that was specified when the database was set up.

   - **Log Folder**. The folder path on the distributor server where the transaction log file for the distribution database will be created.
   - **Distribution Share**. The distribution share folder where replication snapshot files will be generated.
   - **Override Distributor Admin Password**. Select to override the auto-generated replication password which will be used to establish connectivity. The auto-generated password is 14 characters long, and will contain alpha-numeric characters (both upper and lower case) and a special character. If this does not meet the complexity requirements of the server then select this option and specify a password of your choice.
7. When you have set the required replication properties, click **Configure** to configure replication.
8. You may be prompted to save pending changes to the database before continuing. If so, click **Yes** to save pending changes and continue.

9. It may take several minutes to configure replication. Once replication has been configured, the Replication Manager automatically switches to the Monitor tab, which allows you to monitor the progress of the replication snapshot.

9.6.2 Monitor the Replication Snapshot

Note

For a dual sided deployment, the subscriber Database Server is not available for use until the replication snapshot has completed and all the data has been copied from the publisher to the subscriber.

The time taken for the replication snapshot to complete depends on the volume of data in the publisher database and the bandwidth between the servers. For a large database, this may take several hours.

To monitor the progress of the replication snapshot:

1. In the ICE Replication Manager, select the **Monitor** tab. The Monitor tab has the following panes:
   - **Publications** (top left) lists the publisher servers and the publications on each publisher that need to be shared with the subscribers.
   - **Subscriptions and Agents** (top right) shows the subscriptions to a publication and the replication agents associated with a publication. This pane has two tabs, Subscriptions and Agents.
   - **Subscriptions** shows the subscriptions to the selected publication. You can right-click on a subscription to start or stop the subscription.
   - **Agents** shows the replication agents associated with the selected publication. You can right-click on a replication agent to start or stop the agent.
   - **Sessions** (bottom left) shows all sessions for the selected publication and replication agent in the last 24 hours.
   - **Actions** (bottom right) shows the activity for the selected session.
2. In the top left hand pane, select the first Unified CCDM database publication from the list of publications. If you have used the default database name, this will start with **[Portal]**.
3. Wait for the replication snapshot for this publication to complete.

   To check the replication status for a Unified CCDM database publication, in the bottom right hand pane of the Monitor tab, inspect the messages in the

Action Message list. Once the replication snapshot is complete and replication is operational for a publication, you will see the following two messages:

"Delivered snapshot from . . . "

"No replicated transactions are available".

After this, the second message is replaced with messages showing new replicated transactions as they are sent through the system, for example:

"4 transaction(s) with 14 command(s) were delivered".

4. Repeat the two steps above for each of the remaining Unified CCDM database publications.
5. When replication is complete for all portal database publications, close the ICE tool.

The subscriber database can now be used to service requests. For more information about the Replication Manager see the *Administration Guide for Cisco Unified Contact Center Domain Manager*.

9.7 Restart and Validate

9.7.1 Restart the Unified CCDM Services

Following an upgrade it is good practice to restart all Unified CCDM services.

Repeat the following steps on each Unified CCDM Database Server and each and Unified CCDM App/Web Server:

1. Click **Start > Run.**
2. Enter **Services.msc** and then click **OK**.
3. For each Unified CCDM service listed:
   - if the selected service is in the Started state, right click the service name and click **Restart**
   - if the selected service is not started, right-click the service name and click **Start**.

Note

After starting the System Monitoring Service and Application Service on the App/Web Server, you will need to wait a few minutes before logging in to allow the services to load completely.

9.7.2 Validate the Upgrade

Check that the system is functional following the upgrade using the validation tests in section 7.3 "Validating an Upgrade".

10 Split Side Upgrade

10.1 About a Split Sided Upgrade

This chapter describes the steps involved to upgrade a dual-sided deployment, where the upgrade will be split, and one side will be upgraded at a time. Until the second side is upgraded, you will be running two different versions of the software side by side.

This upgrade configuration temporarily breaks the replication and communication channels between the two sides of the system so each side can operate independently as a single-sided system. When replication is restored, the configuration from Side A of the system will replace all configuration on Side B of the system.

Use this mode of operation with caution. Unified CCE and Unified CM changes committed to Side B will be imported from the AW onto Side A, but any Unified CCDM specific configuration items (for example folders, users, security etc.) that are added, changed or deleted on Side B will not be reflected on Side A, even after replication is restored.

This process has two parts.

- Part 1 - split the dual-sided system and upgrade Side A (see section 10.2 "Checklist for Split Side Upgrades Part 1").
- Part 2 - upgrade the split Side B and restore replication (see section 10.8 "Checklist for Split Side Upgrades Part 2").
- The description assumes that you have a two tier deployment (separate database and app/web servers).

Note
Before starting the upgrade please ensure you have the original cryptographic passphrase from the original Unified CCDM installation as you will need it during the upgrade.

10.2 Checklist for Split Side Upgrades Part 1

The first part of the split side upgrade splits the dual-sided system and upgrades Side A.

Step	Complete
Prepare the Unified CCDM servers	
Stop all Unified CCDM Services on the A-Side Unified CCDM servers.	
Remove database replication.	
Backup the Side A and Side B Portal databases.	
Uninstall Existing Unified CCDM Software on Side A	
Uninstall the Database Components from the Side A Database Server	
Uninstall the App/Web Servers Component from the Side A App/Web Server	
Install the new Unified CCDM Components and upgrade the Portal database (Side A)	
Install the new Unified CCDM Database Installer on the Side A Database Server.	
Upgrade the Unified CCDM Portal database on the Side A Database Server.	
Install the Unified CCDM App/Web Servers on the Side A App/Web Servers.	
Finalize Configuration and Restart	
Force failover connections to the active side.	
Update Side B to enable provisioning and import (optional).	
Update provisioning on the Unified CCE AW	
Update provisioning on the Side B Database Server	
Configure the Unified CCE Config Web Service	
Restart (Side A)	
Restart the Unified CCDM Services	

10.3 Prepare the Unified CCDM Servers (Side A)

10.3.1 Stop the Unified CCDM Services (Side A)

Before starting the upgrade stop the Unified CCDM services on all Side A servers.

Data Import Server Service

To stop the Unified CCDM: Data Import Server service, on the Database Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the UCCDM**: Data Import Server** service in the list of services.
4. Select **Stop**.
5. Close the Services window.

Partition Table Manager Service

To stop the Unified CCDM: Partition Table Manager service, on the Database Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the UCCDM**: Partitioning Table Manager** service from the list of services.
4. Select **Stop**.
5. Close the Services window

Provisioning Server Service

To stop the Unified CCDM: Provisioning Server service, on the Database Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the UCCDM**: Provisioning Server** service from the list of services.
4. Select **Stop**.
5. Close the Services window.

System Monitoring Services and Other Services

To stop the remaining Unified CCDM services, on the App/Web Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the Unified CCDM**: System Monitoring Services** service from the list of services.
4. Select **Stop**.

5. At the message: “When UCCDM: System Monitoring Services stops, these other services will also stop. Do you want to stop these services?”, click **Yes**.
6. Close the Services window.

10.3.2 Remove Portal Database Replication

Before the upgrade can proceed, portal database replication must be removed.

To remove portal database replication:

1. Ensure you are logged in to the Side A Database Server as a domain level user with administrative rights over both Database Servers.
2. In your Windows desktop, click **Start > Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment**.
3. The **Database Connection** window is displayed. In this window, set:
   - **Server Name** This option defaults to the current machine.
   - **Database Name** Select the Unified CCDM database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
   - **Authentication** Select Windows Authentication.
4. Click **OK** to open Unified CCDM Integrated Configuration Environment.
5. The Cluster Configuration tool is open by default. From the Tool drop-down list select **Replication Manager**.
6. Click the **Setup** tab to see the replication setup details.
7. Click **Disable** to remove replication from the Unified CCDM database. When prompted, click **Yes** to proceed with replication removal.
8. Replication removal may take several minutes. Wait for the ‘Replication Removed’ message to display in the Output Window and then exit ICE.

10.3.3 Back up the Portal Databases (Side A)

Back up the Unified CCDM Side A Portal database so that you can restore it in the event of a failure.

On the Side A Database Server:

1. Click **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**
2. Connect to the Database Engine using Windows Authentication.
3. Navigate to the Portal database.

4. Right-click **Portal** and select **Tasks > Back Up**.
5. Amend the Destination as appropriate using the Remove and Add features
6. Click **OK**.
7. Close the SQL Server Management Studio window.

10.4 Uninstall Existing Unified CCDM Software on Side A

10.4.1 Uninstall the Database Server Components (Side A)

On the Side A Database Server:

1. Click **Start > Control Panel > Uninstall a program**.
2. In the Programs and Features window, select **Domain Manager: Database Components.**
3. Click **Uninstall** then **Yes** to confirm.The Setup Status window displays, showing the progress of the uninstallation.
4. When the uninstallation is complete, close the Programs and Features window.

10.4.2 Uninstall the App/Web Server Components (Side A)

On the Side A App/Web Server:

1. Click **Start > Control Panel > Uninstall a program**.
2. Select **Domain Manager: Application Server Components.**
3. Click **Uninstall** then **Yes** to confirm.The Setup Status window displays, showing the progress of the uninstallation.
4. When the uninstall is complete, the App/Web Server will reboot automatically.

10.5 Install New Unified CCDM Components and Upgrade Database (Side A)

10.5.1 Install the Database Installer (Side A)

This process does not upgrade the database directly. It just installs the Database Installer which is then used to upgrade the database.

On the Side A Database Server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see section 4.2.1 "About the Unified CCDM Installer").
2. Select **Database Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.
3. When all checks have passed, click **Install** to begin the Database Server Installation. The Setup window displays.
4. Click **Next** to go through each window in turn. You will need to enter the following details:
5. In the License Agreement window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.
6. In the Cryptography Configuration window:
   - **Passphrase.** Enter the cryptographic passphrase you created during installation of the Database Server component when you first installed Unified CCDM. If you continue installation with a new passphrase, you will be unable to access your existing data
   - **Confirm Passphrase.** You will not be able to continue until the contents of this field are identical to the passphrase entered above.

Warning!
You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you do not know the cryptographic passphrase, **stop the installation immediately** and contact your vendor. If you continue the installation with a new passphrase you will be unable to access your existing data.

7. In the Configure Database window:
   - **Database Name**. Enter the name of the database catalog for Unified CCDM. By default this is **Portal**.
   - **Connect Using**. Select the login credentials you want to use:
     - **Windows Authentication Credentials of Application**. This is the recommended option.

- **SQL Server Authentication using the login and password below**. This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your SQL Server Login Name and Password in the fields provided.

- **Click Next.**

8. In the Destination Folder window, you can click **Change** to change the location where the Database components are installed. It is not necessary to install all Unified CCDM components in the same location.
9. Click **Install** to install the Database Installer.

Note
During the Database Install Tool Installation, the J2SE pre-requisite will be automatically installed if it is not already present. You may see a Security Alert dialog box stating that 'Revocation Information for the security certificate for this site is not available'. If so, click **Yes** to continue.

10. To install or upgrade your database immediately after installing the Database Installer, select the **Launch Database Management Utility** check box at the end of the installation before clicking Finish.
11. Click **Finish**.

10.5.2 Upgrade the Portal Database (Side A)

Once the Database Installer is installed, it can be used to upgrade the database.

On the Side A Database Server:

1. If you selected the Launch Database Management Utility check box when you installed the Database Installer, the Database Installer launches automatically after it has been installed. Otherwise, launch the Database Installer manually from **Start > All Programs >** Domain Manager **> Database > Database Installer**. The Database Installer is a wizard which guides you through the steps to upgrade the database.
2. Click **Next** to begin the upgrade process.
3. In the Database Setup Window choose **Upgrade an Existing Database**. Click **Next** to continue.
4. In the SQL Server Connection Details window, take the following actions:

- **Server Name**. Select the Microsoft SQL Server where the Unified CCDM database is located. In this case this is the machine running the application, and so it must be left as the default (local).

- **Database Name**. Enter or select the name of the database catalog that was originally used for the Unified CCDM database.
- **Connect Using**. Select the login credentials you want to use:
  - The **Windows account information you use to log in to your computer**. This is the recommended option.
  - The **Microsoft SQL Server login information assigned by the system administrator**. Only select this option if you are using a database catalog on a different domain. For this option you must enter your Login Name and Password in the fields provided.
- **Test Connection**. Click to make sure the connection to the Microsoft SQL Server is established. If you see the message 'Connection succeeded but database does not exist' then you must rectify this problem before continuing. Check that the database catalog name and security credentials are correct.
- When the database connection details have been tested and the connection is successful, click **Next**.

5. Click **Next** to perform the upgrade. The upgrade may take several minutes.
6. When the Portal database upgrade is complete, click **Close** to close the Database Installer.

10.5.3 Install the App/Web Server (Side A)

Install the new App/Web Server components on the Side A App/Web Servers.

On the Side A Web Server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see section 4.2.1 "About the Unified CCDM Installer").
2. Select **App/Web Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.
3. When all checks have passed, click **Install** to begin the App/Web Server installation. The **Domain Manager: Application Server Component** window displays.
4. Click **Next** to go through each window in turn. You will need to enter the following details:
5. If the Domain Manager: Application Server Components Dialog is displayed, click **Install** to install the additional required components.

6. If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.5 Framework is complete, restart the server to continue the installation of the App/Web Server.
7. In the **License Agreement** window:
   - **I accept the terms in the license agreement**. You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.
8. In the **Cryptography Configuration** window:
   - **Passphrase**. Enter the cryptographic passphrase you created during installation of the Database Server component.
   - **Confirm Passphrase**. You will not be able to continue until the contents of this field are identical to the passphrase entered above.
   - Click **Next** to continue.

Warning!
You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you do not know the cryptographic passphrase, **stop the installation immediately** and contact your vendor. If you continue the installation with a new passphrase you will be unable to access your existing data.

9. In the **Destination Folder** window, you can click **Change** to change the location that the App/Web Server components are installed to. Click **Next** to continue.
10. In the **Configure Database** window:
    - **SQL Server Name**. Enter the host name or IP Address of the server hosting the Unified CCDM database. The default name of **localhost** is only valid if you are installing this component on the Database Server. Otherwise, specify the name of the Database Server. For a dual-sided deployment enter the name of the Side A Database server when installing the Side A components and enter the name of the Side B Database Server when installing the Side B components.
    - **Catalog Name**. Enter or select the database catalog name you specified when installing the Database Server component. If you used the default value, this will be **Portal**.
    - **Connect Using**. Select the login credentials you want to use:
      - **Windows authentication.** This is the recommended option.

- **SQL Server authentication.** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter a SQL Server Login Name and Password in the fields provided.

- Click **Next** to continue.

11. Click **Install**.
12. When the installation has completed, click **Finish**.

Note
The machine will restart once the installation is complete.

10.6 Finalize Configuration (Side A)

10.6.1 Force Failover Connections to the Active Side

To operate the two sides as independent systems, add host file entries to point failover connections to the current active side. This reduces the possibility that a failover will occur to the database on the other side when replication is down.

Since the failover information is held in the database, both sides know about the other side, even though they are currently not replicated or running the same version of Unified CCDM. If a failover occurs then data integrity will be lost. To avoid this, when operating in single-sided mode add the failover connections to the hosts file on each machine to point back to the active side.

For example, in the deployment shown in Figure 10.1 "Host File Entries For Failover in Single-sided Mode", the host file entries are:

Unified CCDM DBA

```
127.0.0.1       Unified CCDM DBB
```

Unified CCDM DBB

```
127.0.0.1      Unified CCDM DBA
```

Unified CCDM WEBA

```
<IP ADDRESS OF Unified CCDM DBA>      Unified CCDM DBB
127.0.0. 1       Unified CCDM WEBB
```

Unified CCDM WEBB

```
<IP ADDRESS OF Unified CCDM DBB>       Unified CCDM DBA
 127.0.0. 1       Unified CCDM WEBA
```

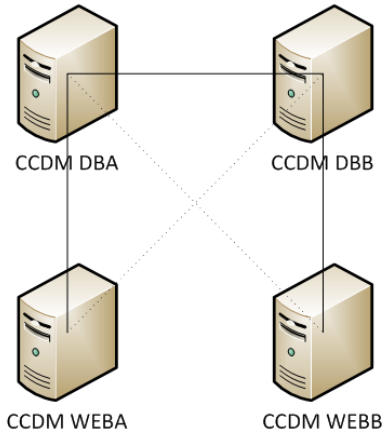

Figure 10.1 Host File Entries For Failover in Single-sided Mode

These entries must be removed once the upgrade is complete and replication between Side A and Side B is restored.

10.6.2 Update Side B to Enable Provisioning and Import (Optional)

If the sides of the system are to be run independently for some time, you may need to enable provisioning and import to run on both Side A and Side B at the same time.

To do this, follow the "Manual Provisioning/Import Failover" steps described in the *Administration Guide for Cisco Unified Contact Center Domain Manager* for the version of Unified CCDM that is currently running on the Side B Database Server.

10.6.3 Update Provisioning on the Unified CCE AW

Update the CMS Control console on the Unified CCE AW to use unique ports for the Side B Provisioning Server.

On the AW:

1. Click **Start > Programs > Cisco Unified CCE Tools > Administration Tools** and select the **CMS Control** application.
2. If the Side B connection exists in the Application Connections then ensure it has different port numbers to the Side A connection.
3. If the Side B connection doesn't exist then make a note of the Side A connection details.
4. Click **Add**.

5. Enter the details as for the Side A but update the Server Name and Hostname details to that of the Side B, and use different port numbers.
6. Click **OK**.
7. Click **Apply**
8. You will be notified that CMSJserver will restart. Please confirm this.

10.6.4 Update Provisioning on the Side B Database Server

To update provisioning on the Side B Database Server, you must change the Side B Provisioning Server ConAPI ports to match those on the Unified CCE AW.

1. On the Side B Database Server, in your Windows desktop, click **Start > Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment**.
2. The Database Connection window is displayed. In this window, set:
   - **Server Name**. This option defaults to the current machine.
   - **Database Name**. Select the Unified CCDM database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
   - **Authentication**. Select **Windows Authentication**.
3. Click **OK** to open Unified CCDM Integrated Configuration Environment.
4. The Cluster Configuration tool is open by default. Select the **Connections** tab on the left hand side.
5. In the list of connections, select the ConAPI connection to the Unified CCE AW. To reduce number of connections shown in the list, so you can find the relevant connection more easily, you may want to click the blue filter arrow on the right hand side of the window near the top, and select the following filter options:
   - Connection Source, Resource Type: **Provisioning Service**
   - Connection Destination, Resource Type: **Cisco CICM**
   - Connection Destination, Component Type: **ConAPI**.
6. On the **Details** tab for the connection, update the port numbers to match those used in the CMS Control Console.
7. To save and action your changes, either click the **Save** icon in the tool bar or select **File> Save** from the menu.
8. You will be informed that the Provisioning Services need to be restarted. Click **OK**.

9. Click **Close**.

10.6.5 Configure the Unified CCE Config Web Service

On the Side A Database Server, the Unified CCE Config Web Service must be configured for each connected Unified CCE Server.

To configure the Unified CCE Config Web Service, on the Side A Database Server:

1. Go to **Start > All Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment**.
2. The **Database Connection** window is displayed. In this window, set:
   - **Server Name**. This option defaults to the current machine.
   - **Database Name**. Select the Unified CCDM database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
   - **Authentication**. Select Windows Authentication.
3. Click **OK** to open Unified CCDM Integrated Configuration Environment.
4. Select the **Setup** tab and click **Configure Cisco Unified CCE Servers** to start the wizard. Click **Next** to go through each window in turn.
5. In the Select Task dialog box select **Modify an existing instance**.
6. Select the Unified CCE instance you want to modify and click **Next**.
7. Complete the dialog boxes as follows:
   - In the Configure Primary Unified Config Web Service dialog box, enter the following details
     - **URL**. This is the auto-generated URL of the primary Unified Config Web Service on the Unified CCE.
     - **User Name**. This is a username with appropriate access to the Unified CCE that the web service is running on. This user must be in the domain security group **<Server>_<UCCE-Instance>_ Config**, where <Server> is the name of the server running Unified CCE and <UCCE-Instance> is the name of the Unified CCE Instance on this server.
     - **Password**. This is the password for the user.
   - In the Configure Primary ConAPI RMI Ports dialog box enter the following ConAPI details:

- **Local Registry Port**. This is the port on the Unified CCE for the Unified CCDM Provisioning service to connect to. This will usually be 2099.
- **Remote Registry Port**. This is the port on the Unified CCDM Database Server for the Unified CCE to connect to. This will usually be 2099.
- **Local Port**. This is selected as the designated port for live provisioning traffic between the Unified CCE and Unified CCDM servers. It must be uniquely assigned for each Unified CCE and any firewalls between the CICM and Unified CCDM server must be configured to allow both-way traffic on this port.

- In the Configure ConAPI Application Instance dialog box enter the following details:
  - **Application Name.** The name of the application to be used for provisioning Unified CCE from Unified CCDM. Specify the name of the application you configured in section 5.3.2 "Set Up ConAPI".
  - **Application Key.** Use the password for the application you specified above.
- In the Multi Media Support dialog box, if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance to provide support for non-voice interactions, select **Yes**. The default is No.
- In the Purge On Delete dialog box, if you want to purge items from Unified CCE automatically when they are deleted from Unified CCDM, select **Yes**. The default is Yes.
- In the Supervisor Active Directory Integration dialog box, if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors, select **Yes**. The default is No. If you select Yes, you will be prompted to provide Active Directory information so that Windows user accounts can be listed.

8. The Summary dialog box summarizes the details of the Unified CCE being configured and the settings you have chosen. Check the details, and if you are satisfied, click **Next**.
9. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.
10. For each remaining Unified CCE Server, click **Configure Cisco Unified CCE Servers**, and repeat the steps above.

11. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu.

10.7 Restart (Side A)

10.7.1 Restart the Unified CCDM Services

Following an upgrade it is good practice to restart all Unified CCDM services.

Repeat the following steps on each Unified CCDM Database Server and each and Unified CCDM App/Web Server:

1. Click **Start > Run.**
2. Enter **Services.msc** and then click **OK**.
3. For each Unified CCDM service listed:
   - if the selected service is in the Started state, right click the service name and click **Restart**
   - if the selected service is not started, right-click the service name and click **Start**.

Note
After starting the System Monitoring Service and Application Service on the App/Web Server, you will need to wait a few minutes before logging in to allow the services to load completely.

10.8 Checklist for Split Side Upgrades Part 2

The second part of the split side upgrade applies the upgrade to Side B and restores replication.

Step	Complete
Prepare the Unified CCDM servers	
Stop all Unified CCDM Services on the B-Side Unified CCDM servers.	
Backup the Side A and Side B Portal databases.	
Uninstall Existing Unified CCDM Software on Side B	
Uninstall the Database Components from the Side B Database Server	

Step	Complete
Uninstall the App/Web Server Components from the Side B App/Web Server	
Install New Components and Upgrade the Portal Database	
Install the Database Installer on the Side B Database Server.	
Do one of the following: • (Option 1) Upgrade the Portal database on the Side B Database Server • (Option 2) Restore the Side B Database from the Side A Database Backup.	
Install the Unified CCDM App/Web Servers on the Side B App/Web Servers.	
Finalize Configuration	
Stop forcing failover connections to the active side.	
Restore Unified CCDM database replication	
Monitor the replication snapshot	
Restart and Validate	
Restart the Unified CCDM Services	
Validate the upgrade	

10.9 Prepare the Unified CCDM Servers (Side B)

10.9.1 Stop the Unified CCDM Services (Side B)

Before starting the upgrade stop the Unified CCDM services on all Side B servers.

Data Import Server Service

To stop the Unified CCDM: Data Import Server service, on the Database Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the UCCDM**: Data Import Server** service in the list of services.
4. Select **Stop**.
5. Close the Services window.

Partition Table Manager Service

To stop the Unified CCDM: Partition Table Manager service, on the Database Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the UCCDM**: Partitioning Table Manager** service from the list of services.
4. Select **Stop**.
5. Close the Services window

Provisioning Server Service

To stop the Unified CCDM: Provisioning Server service, on the Database Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the UCCDM**: Provisioning Server** service from the list of services.
4. Select **Stop**.
5. Close the Services window.

System Monitoring Services and Other Services

To stop the remaining Unified CCDM services, on the App/Web Server:

1. Click **Start > Run**. The Run window displays.
2. In the Open field, enter **services.msc**. The Services window displays.
3. Right-click the Unified CCDM**: System Monitoring Services** service from the list of services.
4. Select **Stop**.
5. At the message: “When UCCDM: System Monitoring Services stops, these other services will also stop. Do you want to stop these services?”, click **Yes**.
6. Close the Services window.

10.9.2 Back up the Portal Database (Side B)

Back up the Unified CCDM Portal database so that you can restore it in the event of a failure.

On the Side B Database Server:

1. Click **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**
2. Connect to the Database Engine using Windows Authentication.
3. Navigate to the Portal database.
4. Right-click **Portal** and select **Tasks > Back Up**.
5. Amend the Destination as appropriate using the Remove and Add features
6. Click **OK**.
7. Close the SQL Server Management Studio window.

10.10 Uninstall Existing Unified CCDM Software(Side B)

10.10.1 Uninstall the Database Server Components (Side B)

On the Side B Database Server:

1. Click **Start > Control Panel > Uninstall a program**.
2. In the Programs and Features window, select **Domain Manager: Database Components.**
3. Click **Uninstall** then **Yes** to confirm.The Setup Status window displays, showing the progress of the uninstallation.
4. When the uninstallation is complete, close the Programs and Features window.

10.10.2 Uninstall the App/Web Server Components (Side B)

On the Side B App/Web Server:

1. Click **Start > Control Panel > Uninstall a program**.
2. Select **Domain Manager: Application Server Components.**
3. Click **Uninstall** then **Yes** to confirm.The Setup Status window displays, showing the progress of the uninstallation.
4. When the uninstall is complete, the App/Web Server will reboot automatically.

10.11 Install New Unified CCDM Components and Upgrade Database (Side B)

10.11.1 Install the Database Installer (Side B)

This process does not upgrade the database directly. It just installs the Database Installer which is then used to upgrade the database.

On the Side B Database Server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see section 4.2.1 "About the Unified CCDM Installer").
2. Select **Database Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.
3. When all checks have passed, click **Install** to begin the Database Server Installation. The Setup window displays.
4. Click **Next** to go through each window in turn. You will need to enter the following details:
5. In the License Agreement window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.
6. In the Cryptography Configuration window:
   - **Passphrase.** Enter the cryptographic passphrase you created during installation of the Database Server component when you first installed Unified CCDM. If you continue installation with a new passphrase, you will be unable to access your existing data
   - **Confirm Passphrase.** You will not be able to continue until the contents of this field are identical to the passphrase entered above.

Warning!
You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you do not know the cryptographic passphrase, **stop the installation immediately** and contact your vendor. If you continue the installation with a new passphrase you will be unable to access your existing data.

7. In the Configure Database window:

- **Database Name**. Enter the name of the database catalog for Unified CCDM. By default this is **Portal**.
- **Connect Using**. Select the login credentials you want to use:
  - **Windows Authentication Credentials of Application**. This is the recommended option.
  - **SQL Server Authentication using the login and password below**. This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your SQL Server Login Name and Password in the fields provided.
- **Click Next.**

8. In the Destination Folder window, you can click **Change** to change the location where the Database components are installed. It is not necessary to install all Unified CCDM components in the same location.
9. Click **Install** to install the Database Installer.

Note
During the Database Install Tool Installation, the J2SE pre-requisite will be automatically installed if it is not already present. You may see a Security Alert dialog box stating that 'Revocation Information for the security certificate for this site is not available'. If so, click **Yes** to continue.

10. To install or upgrade your database immediately after installing the Database Installer, select the **Launch Database Management Utility** check box at the end of the installation before clicking Finish.
11. Click **Finish**.

10.11.2 About Upgrading the Side B Database

There are two options for upgrading the Side B database in a split-sided upgrade. Once you have installed the database installer, you can upgrade the Side B database directly, or you can restore it from the Side A backup.

- Option 1: Upgrade the Side B database directly. If the system has been running in single-sided mode for less than 24 hours, then we recommend that you choose this option. Follow the instructions in section 10.11.3 "Upgrade Side B Database (Option 1)".
- Option 2: Restore the Side B database from the Side A backup. If the system has been running in single-sided mode for more than 24 hours, then we recommend that you restore the Side B database from the Side A backup that

- you made when you started part 2 of the split-sided upgrade. Follow the instructions in section 10.11.4 "Restore Side B Database from the Side A Backup (Option 2)".

10.11.3 Upgrade Side B Database (Option 1)

Choose the option if your system has been running in single-sided mode for less than 24 hours.

On the Side B Database Server:

1. If you selected the Launch Database Management Utility check box when you installed the Database Installer, the Database Installer launches automatically after it has been installed. Otherwise, launch the Database Installer manually from **Start > All Programs >** Domain Manager **> Database > Database Installer**. The Database Installer is a wizard which guides you through the steps to upgrade the database.
2. Click **Next** to begin the upgrade process.
3. In the Database Setup Window choose **Upgrade an Existing Database**. Click **Next** to continue.
4. In the SQL Server Connection Details window, take the following actions:
   - **Server Name**. Select the Microsoft SQL Server where the Unified CCDM database is located. In this case this is the machine running the application, and so it must be left as the default (local).
   - **Database Name**. Enter or select the name of the database catalog that was originally used for the Unified CCDM database.
   - **Connect Using**. Select the login credentials you want to use:
     - The **Windows account information you use to log in to your computer**. This is the recommended option.
     - The **Microsoft SQL Server login information assigned by the system administrator**. Only select this option if you are using a database catalog on a different domain. For this option you must enter your Login Name and Password in the fields provided.
   - **Test Connection**. Click to make sure the connection to the Microsoft SQL Server is established. If you see the message 'Connection succeeded but database does not exist' then you must rectify this problem before continuing. Check that the database catalog name and security credentials are correct.
   - When the database connection details have been tested and the connection is successful, click **Next**.
5. Click **Next** to perform the upgrade. The upgrade may take several minutes.

6. When the Portal database upgrade is complete, click **Close** to close the Database Installer.

10.11.4 Restore Side B Database from the Side A Backup (Option 2)

Choose this option if your system has been running in single-sided mode for more than 24 hours. This will ensure that audit information is consistent across both sides. In this option, you will restore the Side B portal database from the backup of the Side A portal database.

Locate the backup of the Side A portal database, then, on the Side B Database Server:

1. Click **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
2. Right-click the **Databases** folder and click **Restore Database**.
3. In the Restore Database window choose **From Device**, click **Add** and add the location of the database back up file you want to restore from. You may need to copy the backup file to a local file in order to access it. Click **OK**.
4. Select the check box next to the backup set you just added.
5. From the **To Database** drop-down list, select the **Portal** database as the restore destination.
6. Select **Options** and choose **Overwrite the existing database**. This will restore the database to the same location as the previous database. If you would like to choose a different location, update the **Restore As** path for each file to your preferred data file location.
7. Click **OK** to start the restore.

10.11.5 Install the Unified CCDM App/Web Server (Side B)

Install the new App/Web Server components on the Side B App/Web Server.

On the Side B Web Server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see section 4.2.1 "About the Unified CCDM Installer").
2. Select **App/Web Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.
3. When all checks have passed, click **Install** to begin the App/Web Server installation. The **Domain Manager: Application Server Component** window displays.

4. Click **Next** to go through each window in turn. You will need to enter the following details:
5. If the Domain Manager: Application Server Components Dialog is displayed, click **Install** to install the additional required components.
6. If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.5 Framework is complete, restart the server to continue the installation of the App/Web Server.
7. In the **License Agreement** window:
   - **I accept the terms in the license agreement**. You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.
8. In the **Cryptography Configuration** window:
   - **Passphrase**. Enter the cryptographic passphrase you created during installation of the Database Server component.
   - **Confirm Passphrase**. You will not be able to continue until the contents of this field are identical to the passphrase entered above.
   - Click **Next** to continue.

Warning!
You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you do not know the cryptographic passphrase, **stop the installation immediately** and contact your vendor. If you continue the installation with a new passphrase you will be unable to access your existing data.

9. In the **Destination Folder** window, you can click **Change** to change the location that the App/Web Server components are installed to. Click **Next** to continue.
10. In the **Configure Database** window:
    - **SQL Server Name**. Enter the host name or IP Address of the server hosting the Unified CCDM database. The default name of **localhost** is only valid if you are installing this component on the Database Server. Otherwise, specify the name of the Database Server. For a dual-sided deployment enter the name of the Side A Database server when installing the Side A components and enter the name of the Side B Database Server when installing the Side B components.

- **Catalog Name**. Enter or select the database catalog name you specified when installing the Database Server component. If you used the default value, this will be **Portal**.
- **Connect Using**. Select the login credentials you want to use:
  - **Windows authentication.** This is the recommended option.
  - **SQL Server authentication.** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter a SQL Server Login Name and Password in the fields provided.
- Click **Next** to continue.

11. Click **Install**.
12. When the installation has completed, click **Finish**.

Note
The machine will restart once the installation is complete.

10.12 Finalize Configuration (Side B)

10.12.1 Stop Forcing Failover Connections to the Active Side

To stop forcing the failover connections to the active side:

1. Remove the entries you made in section 10.6.1 "Force Failover Connections to the Active Side" to the **hosts** files on all servers.

10.12.2 Restore Unified CCDM Database Replication

For a dual-sided deployment, you must reinstate replication between the Side A and Side B portal databases. Replication between the databases is set up and monitored using the Replication Manager application which is available in the Unified CCDM Integrated Configuration Environment (ICE) tool.

Note
The user running Replication Manager must have administrator permissions in both Windows and SQL Server, for both the publisher and the subscriber Database Servers.

Usually, the publisher will be the Side A Database Server, but occasionally, it may be necessary to configure the Side B Database Server as the publisher.

To configure replication, on the publisher Database Server:

1. Go to **Start > All Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment**.
2. The **Database Connection** window is displayed. In this window, set:
   - **Server Name**. This option defaults to the current machine.
   - **Database Name**. Select the Unified CCDM database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
   - **Authentication**. Select Windows Authentication.
3. Click **OK** to open ICE. The ICE Cluster Configuration tool starts by default.
4. From the Tool drop-down list, select **Replication Manager**. The Replication Manager opens in the Setup tab. The Setup tab has the following sections:
   - **Unified CCDM Database Server Properties** contains the publisher and subscriber Unified CCDM database details.
   - **Distributor Properties** contains the SQL Server Replication distributor properties.

   The default values shown in the Setup tab are derived from the values initially configured in the Cluster Configuration tool and will be suitable in most cases.
5. If required, modify the Unified CCDM Database Server Properties.
   - **Server Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.
   - **Catalog Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration. It may be changed, but if so, a valid database with the new name must already exist on the corresponding server.
6. If required, modify the distributor properties.
   - **Server Name**. The name of the subscriber server hosting the Unified CCDM database. This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.
   - **Catalog Name**. The name to be assigned to the distribution database. The recommended value is **distribution_portal**.
   - **Data Folder**. The folder path on the distributor server where the data file for the distribution database will be created.

Note

If you are setting up replication after performing an upgrade, be particularly careful with the Data Folder path, as it may be different from the value used in previous versions of Unified CCDM. Make sure you use the path that was specified when the database was set up.

- **Log Folder**. The folder path on the distributor server where the transaction log file for the distribution database will be created.
- **Distribution Share**. The distribution share folder where replication snapshot files will be generated.
- **Override Distributor Admin Password**. Select to override the auto-generated replication password which will be used to establish connectivity. The auto-generated password is 14 characters long, and will contain alpha-numeric characters (both upper and lower case) and a special character. If this does not meet the complexity requirements of the server then select this option and specify a password of your choice.

7. When you have set the required replication properties, click **Configure** to configure replication.
8. You may be prompted to save pending changes to the database before continuing. If so, click **Yes** to save pending changes and continue.
9. It may take several minutes to configure replication. Once replication has been configured, the Replication Manager automatically switches to the Monitor tab, which allows you to monitor the progress of the replication snapshot.

10.12.3 Monitor the Replication Snapshot

Note

For a dual sided deployment, the subscriber Database Server is not available for use until the replication snapshot has completed and all the data has been copied from the publisher to the subscriber.

The time taken for the replication snapshot to complete depends on the volume of data in the publisher database and the bandwidth between the servers. For a large database, this may take several hours.

To monitor the progress of the replication snapshot:

1. In the ICE Replication Manager, select the **Monitor** tab. The Monitor tab has the following panes:

- **Publications** (top left) lists the publisher servers and the publications on each publisher that need to be shared with the subscribers.
- **Subscriptions and Agents** (top right) shows the subscriptions to a publication and the replication agents associated with a publication. This pane has two tabs, Subscriptions and Agents.
- **Subscriptions** shows the subscriptions to the selected publication. You can right-click on a subscription to start or stop the subscription.
- **Agents** shows the replication agents associated with the selected publication. You can right-click on a replication agent to start or stop the agent.
- **Sessions** (bottom left) shows all sessions for the selected publication and replication agent in the last 24 hours.
- **Actions** (bottom right) shows the activity for the selected session.

2. In the top left hand pane, select the first Unified CCDM database publication from the list of publications. If you have used the default database name, this will start with **[Portal]**.
3. Wait for the replication snapshot for this publication to complete.

   To check the replication status for a Unified CCDM database publication, in the bottom right hand pane of the Monitor tab, inspect the messages in the Action Message list. Once the replication snapshot is complete and replication is operational for a publication, you will see the following two messages:

   "Delivered snapshot from . . . "

   "No replicated transactions are available".

   After this, the second message is replaced with messages showing new replicated transactions as they are sent through the system, for example:

   "4 transaction(s) with 14 command(s) were delivered".
4. Repeat the two steps above for each of the remaining Unified CCDM database publications.
5. When replication is complete for all portal database publications, close the ICE tool.

The subscriber database can now be used to service requests. For more information about the Replication Manager see the *Administration Guide for Cisco Unified Contact Center Domain Manager*.

10.13 Restart and Validate (Side B)

10.13.1 Restart the Unified CCDM Services

Following an upgrade it is good practice to restart all Unified CCDM services.

Repeat the following steps on each Unified CCDM Database Server and each and Unified CCDM App/Web Server:

1. Click **Start > Run.**
2. Enter **Services.msc** and then click **OK**.
3. For each Unified CCDM service listed:
   - if the selected service is in the Started state, right click the service name and click **Restart**
   - if the selected service is not started, right-click the service name and click **Start**.

Note
After starting the System Monitoring Service and Application Service on the App/Web Server, you will need to wait a few minutes before logging in to allow the services to load completely.

10.13.2 Validate the Upgrade

Check that the system is functional following the upgrade using the validation tests in section 7.3 "Validating an Upgrade".

11 Uninstalling Unified CCDM

11.1 About Uninstalling Unified CCDM

This chapter describes how to remove the Unified CCDM components from the platform.

To uninstall Unified CCDM, firstly you must remove the database components. This removes the ability to import and provision data between remote data sources (such as Unified CCE or Unified CM) and the Unified CCDM Database.

Uninstallation involves the following steps:

- removing database replication (dual-sided systems only)
- uninstalling the database components
- removing the database catalog (only if Unified CCDM is being removed permanently)
- uninstalling the other Unified CCDM components.

11.2 Remove Database Replication

Note
This step is only required if you have a dual-sided system.

If you have a dual-sided installation then you must remove database replication before removing the database components.

Before removing database replication:

1. Ensure that the database is in a consistent state.
2. Stop all Unified CCDM Services on all servers.

To remove portal database replication:

1. Ensure you are logged in to the Side A Database Server as a domain level user with administrative rights over both Database Servers.
2. In your Windows desktop, click **Start > Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment**.
3. The **Database Connection** window is displayed. In this window, set:
   - **Server Name** This option defaults to the current machine.

- **Database Name** Select the Unified CCDM database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
- **Authentication** Select Windows Authentication.

4. Click **OK** to open Unified CCDM Integrated Configuration Environment.
5. The Cluster Configuration tool is open by default. From the Tool drop-down list select **Replication Manager**.
6. Click the **Setup** tab to see the replication setup details.
7. Click **Disable** to remove replication from the Unified CCDM database. When prompted, click **Yes** to proceed with replication removal.
8. Replication removal may take several minutes. Wait for the 'Replication Removed' message to display in the Output Window and then exit ICE.

11.3 Uninstall the Database Components

To uninstall the database components, on the Database Server:

1. Click **Start > Control Panel > Uninstall a program.**
2. Select **Domain Manager: Database Components.**
3. Click **Uninstall.**

For a dual-sided deployment, repeat these steps on the Side B Database Server.

Note
Uninstalling the database components does not remove the Unified CCDM database catalog.

11.4 Remove the Database Catalog

Warning!
Do not remove the database catalog from your system unless you intend to permanently remove Unified CCDM, or you have been instructed to do so by your vendor support.

To remove the Unified CCDM database catalog, you will need to use SQL Server Management Studio, as follows:

1. Click **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**

2. Connect to the local Database Server.
3. In the Object Explorer pane, expand the **Databases** node, navigate to the Unified CCDM database (the default name is Portal), right click it and select **Delete**.
4. The Delete Database window displays.
5. Select the **Close existing connections** check box.
6. Click **OK**.

This permanently removes the database catalog.

11.5 Uninstall the Other Components

To uninstall the other Unified CCDM components:

1. On the App/Web Server, click **Start > Control Panel > Uninstall a program.**
2. Select **Domain Manager: Application Server Components.**
3. Click **Uninstall.**
4. For a dual-sided deployment, repeat step 1. to step 3. on the Side B App/Web Server.
5. On the OLAP Server, click **Start > Control Panel > Uninstall a program.**
6. Select **Domain Manager: OLAP Components.**
7. Click **Uninstall.**
8. For a dual-sided deployment, repeat step 5. to step 7. on the Side B OLAP Server.

12 Troubleshooting

12.1 About Installer Logs

Unified CCDM installers are launched with logging enabled. Install logs are located in **C:\InstallLogs** for both the Database and App/Web Server installers.