# Installation Guide for Cisco Unified Contact Center Management Portal

# Release 8.5(2)

**July 2011**

**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

# Contents


**Preface** ..... v

**Purpose** ..... v

**Audience** ..... v

**Organization** ..... v

**Related Documentation** ..... vi

**Product Naming Conventions** ..... vii

**Conventions** ..... viii

**Obtaining Documentation and Submitting a Service Request** ..... ix

**Documentation Feedback** ..... ix

**1. Cisco Unified Contact Center Management Portal** ..... 1

**Primary Functionality** ..... 1

**Deployment Specifics** ..... 2

**Deployment Models** ..... 3
Unified CCMP Architecture ..... 3

**2. Installation Guidelines and Requirements** ..... 5

**Installation Prerequisite Checklist** ..... 5
Database Server Prerequisites ..... 5
Web/Application Server Prerequisites ..... 5
Obtaining the Prerequisites ..... 6

**General Advice** ..... 6

**Backup Guidelines** ..... 7

**Server Requirements** ..... 7
Microsoft Windows ..... 7

**Required Domain User Accounts** ..... 9

**3. Microsoft SQL Server Setup** ..... 10

**Overview** ..... 10

**Microsoft SQL Server Component Installation** ..... 10

**Installing SQL Server for a Single Server Deployment ..... 11**
Installation ..... 11
SQL Server 2005 Database Server Configuration ..... 13
SQL Server 2005 Reporting Services Configuration ..... 13

**Installing SQL Server for a Two-Tier Deployment ..... 15**
Database Server: SQL Server Installation ..... 15
Database Server: SQL Server Configuration ..... 16
Configuring Windows 2008 R2 Firewall for SQL Server ..... 17
Web Server: SQL Server Installation ..... 18
Web Server: SQL Server Configuration ..... 19

**4. Component Installation ..... 23**

**Planning Your Installation ..... 23**

**Recording Your Settings ..... 23**

**Component Installation ..... 24**
Component Installation using the Unified CCMP CD ..... 24

**Database Component ..... 25**
Database Install Tool Installation ..... 25
Database Setup ..... 26

**Application Server Component ..... 28**
Application Server Component Installation ..... 28

**Web Server Component ..... 29**
Web Server Component Installation ..... 29

**Data Import Server Component ..... 30**
Data Import Server Component Installation ..... 30

**Provisioning Server Component ..... 31**
Provisioning Server Component Installation ..... 31

**Diagnostic Framework ..... 31**
Diagnostic Framework Installation ..... 31

**5. Component Configuration ..... 33**

**Unified CCMP Cluster Configuration Overview ..... 33**

**AWDB Database Security Configuration ..... 34**

**Common ConAPI Credentials ..... 34**

**CMS Server Setup ..... 35**

**Unified CCMP Configuration Procedure ..... 36**
Physical Servers ..... 37
UCCMP Servers ..... 37

Communications Servers ..... 42
Connection Manager ..... 47
Global Properties ..... 47
Saving the Configuration ..... 48

**6. Post-Installation Steps ..... 49**

**Starting the Unified CCMP Services ..... 49**

**Logging in to Unified CCMP ..... 49**

**Report Uploading ..... 50**

**Unified CVP Media File Upload ..... 50**
Preparing the Configuration ..... 50
Configuring Distributed File System for Unified CVP Media File Upload 51
Configuring DFS Root Targets ..... 51
Configuring File Replication for Unified CVP Media File Upload ..... 52

**Support for Additional Languages ..... 52**

**Validating the Unified CCMP Installation ..... 53**

**Security Hardening ..... 55**

**7. Upgrading from a Previous Version ..... 56**

**Overview ..... 56**
Upgrade Checklist ..... 56

**Upgrade Procedure ..... 58**
Before Upgrading ..... 58
Installing Unified CCMP ..... 63
Unified CCMP Configuration ..... 68

**8. Platform Uninstallation ..... 73**

**Uninstalling the Data Import Server and Provisioning Components ..... 73**
Removing Replication ..... 73
Uninstalling the Provisioning Server Component ..... 74

**Uninstalling the Database Component ..... 74**

**Uninstalling All Other Components ..... 75**

**9. Troubleshooting ..... 76**

**Installing Unified CCMP Components with Logging Enabled ..... 76**

**Adding a New Web Server After the Database Is Installed ..... 76**

**Upgrade Troubleshooting** ..... **78**
SQL Server 2005 Reporting Services Upgrade Troubleshooting ..... 78

**Glossary** ..... **80**

**Index** ..... **83**

# Preface

## Purpose

This document explains how to install the Cisco Unified Contact Center Management Portal (Unified CCMP) components.

## Audience

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

## Organization

The following table describes the information contained in each chapter of this guide.

| Chapter | Description |
|---|---|
| Chapter 1, Cisco Unified Contact Center Management Portal<br>Intended Audience: All audiences | Introduces Unified CCMP, including its integration with Unified CCE. |
| Chapter 2, Installation Guidelines and Requirements<br>Intended Audience: System administrators | Lists the prerequisites for Unified CCMP installation and provides recommendations for pre installation platform configuration. |
| Chapter 3, Microsoft SQL Server Setup<br>Intended Audience: System administrators with Microsoft SQL Server experience | Describes how to setup the Microsoft SQL Server. |
| Chapter 4, Component Installation<br>Intended Audience: System administrators | Provides instructions for the installation of all Unified CCMP components. |
| Chapter 5, Component Configuration<br>Intended Audience: System administrators | Describes post-installation configuration of Unified CCMP, including setting up replication and uploading .wav files for voice announcements. The procedure for configuring a Unified CCMP server cluster is detailed as well as how to use the Unified CCMP Configuration Manager to replicate data between Database servers. Web and Database component server performance checklists are also provided. |
| Chapter 6, Post-Installation Steps<br>Intended Audience: System administrators | Describes how to set the administrator password for, and upload report templates into, Unified CCMP platform. |
| Chapter 7, Upgrading from a Previous Version<br>Intended Audience: System administrators | Explains how to upgrade from an existing installation of Unified CCMP to the latest version without losing your data. |

| Chapter | Description |
|---|---|
| Chapter 8, Platform Uninstallation.<br>Intended Audience: System administrators | Describes how to remove Unified CCMP platform from your servers. |
| Chapter 9, Troubleshooting | Describes how to enable logging for the Unified CCMP 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 Contact Center Management Portal, 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** > **Customer Contact** > **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: Unified ICM/IPCC* available at (login 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.

## Product Naming Conventions

In this release, the product names defined in the table below have changed. The New Name (long version) is reserved for the first instance of that product name and in all headings. The New Name (short version) is used for subsequent instances of the product name.

**Note:** This document uses the naming conventions provided in each GUI, which means that in some cases the old product name is in use.

| Old Product Name | New Name (long version) | New Name (short version) |
|---|---|---|
| Cisco IPCC Enterprise Edition | Cisco Unified Contact Center Enterprise | Unified CCE |
| Cisco System IPCC Enterprise Edition | Cisco Unified System Contact Center Enterprise | Unified SCCE<br>**Note:** Cisco Unified System Contact Center Enterprise (Unified SCCE) is supported in 8.5(2); however, there is not a separate 8.5(2) version. If you request features that are in 8.5(2), you must migrate to the Unified ICM/CCE/CCH software. Full migration information is documented in the *Upgrade Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*. |
| Cisco IPCC Hosted Edition | Cisco Unified Contact Center Hosted | Unified CCH |
| Cisco Intelligent Contact Management (ICM) Enterprise Edition | Cisco Unified Intelligent Contact Management (ICM) Enterprise | Unified ICM |
| Cisco Intelligent Contact Management (ICM) Hosted Edition | Cisco Unified Intelligent Contact Management (ICM) Hosted | |
| Cisco Call Manager/Cisco Unified Call Manager | Cisco Unified Communications Manager | Unified CM |

## Conventions

This manual 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:<br>• Chose **Edit > Find**.<br>• Click **Finish** |
| *italic* font | Italic font is used to indicate the following:<br>• To introduce a new term; for example: A *skill group* is a collection of agents who share similar skills.<br>• For emphasis; for example: *Do not* use the numerical naming convention.<br>• A syntax value that the user must replace; for example: IF (*condition*, *true-value*, *false-value*)<br>• A book title; for example: Refer to the *Cisco CRS Installation Guide* |
| `window font` | Window font, such as Courier, is used for the following:<br>• Text as it appears in code or that the window displays: for example: **<html><title>Cisco Systems, Inc. </title></html>**<br>• Navigational text when selecting menu options; for example **Configuration Manager > Tools > Explorer Tools > Agent Explorer** |
| < > | Angle brackets are used to indicate the following:<br>• For arguments where the context does not allow italic, such as ASCII output<br>• A character string that the user enters, but does not appear in the window such as a password |

## Obtaining Documentation and Submitting a Service Request

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

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

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

## Documentation Feedback

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

ccbu_docfeedback@cisco.com

We appreciate your comments.

# 1. Cisco Unified Contact Center Management Portal

Cisco Unified Contact Center Management Portal (Unified CCMP) is a suite of components that form part of Cisco Unified Contact Center Enterprise (Unified CCE) and hosted deployments of Unified CCE. Unified CCMP serves three mutually supportive purposes:

- **Simplifies** the operations and procedures for performing basic tasks such as adding or modifying Agents, Skill Groups, Teams and other common administrative functions.
- Provides a **common web user interface** to the product set. Currently, Unified CCE, hosted deployments of Unified CCE and Unified Communications Manager (Unified CM) use different interfaces. Simple tasks, such as adding an agent, therefore require performing multiple operations in several applications to achieve a single goal. By providing a web-based unified interface for common administrative tasks, Unified CCMP decreases the amount of time, knowledge, training, and resources required to administer the solution set.
- Provides an **audit trail** for changes made through Unified CCE and hosted deployments of Unified CCE. Through the supplied audit reports or the individual resource histories, administrators and other power users can trace the timing of, and the person responsible for, provisioning changes.

Unified CCE and hosted deployments of Unified CCE customers can optionally deploy Unified CCMP to satisfy particular business requirements.

## Primary Functionality

**Note:** For ease of reading the term Unified CCE includes hosted deployments of Unified CCE, unless hosted deployments of CCE are specifically required.

Unified CCMP provides *Unified Configuration*, that is, the provisioning of the applicable Unified CCE components through a single task-based web interface.

Unified CCMP provides users with the following functionality:

- Hierarchical Administration allowing you to:
  - Service Provider Administrator can add a Portal User.
  - Tenant Administrator can add a Skill Group.
  - Tenant Supervisor can add an Agent.

  **Note:** These permissions are completely configurable.
- Perform **Audit Trails** on configuration changes and usage.

In terms of configuration, Unified CCMP differentiates between commissioning and provisioning.

- **Commissioning** consists of operations that install and initially configure a system of components. These operations are typically done by the Service

Provider using existing setup and configuration tools. An example operation is setting up and configuring a peripheral.

- **Provisioning** consists of day-to-day configuration operations performed by a tenant. Examples include creating or modifying Agents, Skill Groups and Agent Teams.

Service Providers use the existing Unified CCE, Unified CM, and Unified CVP installers and configuration tools to commission a system. They then install Unified CCMP and use it to define organizational units and to set up permissions. The organizational units can then use Unified CCMP to provision their specific site.

Unified CCMP uses its own database to provide a virtualization layer between Unified CCE and the user. This allows resources to be organized as best suits business needs, irrespective of the underlying organization of Unified Contact Center. Resources can then be provisioned or edited in Unified CCMP from a single user interface, and Unified CCMP performs all the necessary provisioning tasks to add them to Unified CCE.

Additionally, Unified CCMP can read existing configuration data from Unified CCE and Unified CM, store it in the Unified CCMP database and reconcile differences between the two. This enables Service Providers to make configuration changes using existing Unified CCE and Unified CM tools. These changes are automatically propagated into Unified CCMP.

## Deployment Specifics

Unified CCMP deployments are limited to standard Unified CCE, or Cisco Unified System Contact Center Enterprise (Unified SCCE) deployments with the following restrictions:

- Each Tenant must have its own:
  - Unified ICM instance.
  - Dedicated Administration & Data Server Real Time Distributor server. Multiple Distributor instances on a single server are not allowed.
  - Dedicated Administration & Data Server CMS Server. Multiple CMS Server instances on a single server are not allowed.
- Unified CCMP is only supported on Unified CCE 7.1 and later and Unified SCCE 7.5.

## Deployment Models

In many environments, Unified CCMP 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 web/application servers are separated by a demilitarized zone (DMZ).

Because Unified CCMP 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 CCMP components are installed on a single dedicated server. This system can manage **150 Portal users**.
- **Two Tier (Secure Deployment)**. Unified CCMP Application, Web, and Reporting components are hosted on one server. The Provisioning, Data Import and Database components are hosted on a second server. This system can manage **800 Portal users**.

### Unified CCMP Architecture

A Unified CCMP installation comprises the following components.

- **Database Server** The Portal database stores configuration and audit information.
- **Application Server** The application server delivers application services such as search and security to the Unified CCMP Web Server.
- **Web Server** The web server is the Unified CCMP front end through which users gain access to the application.
- **Data Import Server** the Data Import Server imports configuration items and changes to configuration items such as agents, call types and skill groups from Unified CCE.
- **Provisioning Server** the Provisioning Server applies configuration changes submitted by Unified CCMP users to Unified CCE.

Depending on the deployment model chosen the components may reside on different servers.

Figure 1, below, describes the software installation layout for a single tier deployment. All components reside on a single server. Optionally, a second side can be included for resilience.

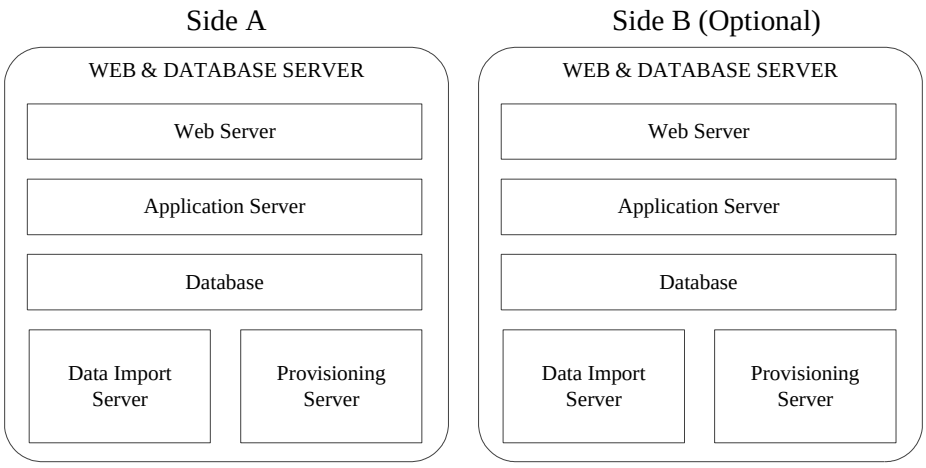


**Figure 1: Unified CCMP software component layout for a single tier deployment.**

Figure 2, below, describes the software installation layout for a dual tier deployment. The web server and application server components reside on a separate server. Optionally, a second side can be included for resilience.

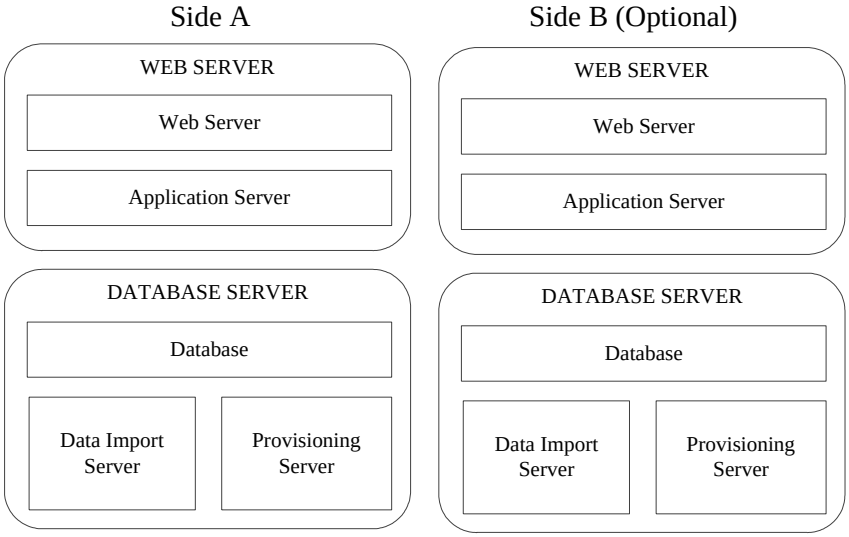


**Figure 2: Unified CCMP software component layout for a dual tier deployment.**

# 2. Installation Guidelines and Requirements

## Installation Prerequisite Checklist

To operate correctly, each Unified CCMP component requires that its prerequisite software be installed. A mandatory check is performed before each part of the installation. The installation will not proceed if this check does not find the required software.

You must therefore install the prerequisites on the appropriate servers prior to starting any part of the installation.

A summary of these prerequisites is listed below. Detailed instructions for installation of the SQL Server components are included in section 3, Microsoft SQL Server Setup.

### Database Server Prerequisites

- Windows Server 2008 R2 Standard Edition (64-bit)
    - Microsoft .NET Framework 3.5 SP1 feature added
- J2SE Runtime Environment 6.0, Update 11 (64-bit)
- Microsoft SQL Server 2005 Standard or Enterprise Edition (32-bit):
    - Database Server Components
    - Workstation Components
- Microsoft SQL Server 2005 SP4
- Microsoft SQL Server 2005 SMO for 64-bit (Microsoft SQL Server 2005 Management Objects Collection)

### Web/Application Server Prerequisites

- Windows Server 2008 R2 Standard Edition (64-bit)
    - Application Server Role configured
        - Microsoft .NET Framework 3.5 SP1 feature added
        - Web Server (IIS) role service added
- Microsoft ASP.NET 2.0 AJAX Extensions 1.0
- Microsoft WSE 2.0 SP3 (runtime only)
- Microsoft SQL Server 2005 Standard or Enterprise Edition (32-bit):
    - Reporting Services Components
    - Workstation Components
- Microsoft SQL Server 2005 SP4

In a small scale deployment where all Unified CCMP components will be installed on a single server, all of the above prerequisites should be present on the single server.

### Obtaining the Prerequisites

**Microsoft .NET Framework 3.5 SP1** is included as a feature of Microsoft Windows Server 2008 R2. See the Server Requirements section below for instructions on enabling the feature.

**Microsoft ASP.NET 2.0 AJAX Extensions 1.0** can be downloaded from the following location:

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=ca9d90fa-e8c9-42e3-aa19-08e2c027f5d6&displaylang=en

**Microsoft WSE 2.0 SP3** can be downloaded from the following location:

http://www.microsoft.com/downloads/en/details.aspx?familyid=1ba1f631-c3e7-420a-bc1e-ef18bab66122&displaylang=en

**SQL Server Service Pack 4** can be downloaded from the following location:

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=b953e84f-9307-405e-bceb-47bd345baece

**J2SE Runtime Environment 6.0, Update 11 (64-Bit)** can be downloaded from the following location:

http://java.sun.com/products/archive/j2se/6u11/index.html

**Microsoft SQL Server 2005 SMO for 64-bit (Microsoft SQL Server 2005 Management Objects Collection)** can be downloaded from the following location:

http://download.microsoft.com/download/4/4/D/44DBDE61-B385-4FC2-A67D-48053B8F9FAD/SQLServer2005_XMO_x64.msi

## General Advice

- Install the pre-requisite software and the Unified CCMP application while logged in using a *domain account* with *administrative* privileges over all of the platform machines.
- Antivirus software may state that the **autorun.hta** script file which launches the installer when the installation media is inserted is malicious. If this message

displays during installation, you can safely ignore it and continue with the installation.

- Install Microsoft Internet Explorer (IE) 6 SP2, IE 7 or IE 8 on all the machines from which the Unified CCMP website will be accessed.
- Harden the Internet Information Services Web Server (IIS) and Microsoft SQL Server 2005 according the latest Microsoft guidelines.
- Disable all unnecessary local services (FTP, BITS and so on).
- Use Microsoft Terminal Services for remote configuration and support.

## Backup Guidelines

- Ensure that the Unified CCMP Portal database is set to Simple recovery mode in the database properties window of SQL Server 2005 Management Studio. Also ensure that the global Recovery Interval setting is set to 0 for the SQL Server. This setting can be configured in the Server Properties section of SQL Server 2005 Management Studio.
- Regularly back up the Microsoft SQL Server databases and truncate transaction logs to prevent them becoming excessively large.
- Schedule backups for quiet times of the day.

## Server Requirements

### Microsoft Windows

The following rules apply to all servers upon which Unified CCMP will be installed.

- Do NOT install Unified CCMP on a domain controller.
- Only use alphanumeric characters in Portal server names, without underscores.
- All Unified CCMP servers must be configured to use the U.S. English character set.

#### User Access Control

User Account Control (UAC) is a Windows feature that was introduced to protect the operating system from malicious programs. UAC must be disabled on all servers before Unified CCMP installation begins. To disable UAC perform the following steps:

1. Click **Start > Control Panel > User Accounts**.
2. Click **User Accounts**, and then open **Change User Account Control settings**.
3. Use slide bar to select **Never Notify** option to disable UAC.
4. Click **OK**.
5. You must restart your machine to commit the new UAC settings.

UAC can be safely re-enabled after Unified CCMP installation is complete.

### Disable FIPS Compliance Checking

Ensure that FIPS compliance checking is disabled on all servers upon which Unified CCMP will be installed.

1. Click **Start > All Programs > Administrative Tools > Local Security Policy**. The Local Security Policy tool is displayed.
2. Click the **Local Policies** folder and click **Security Options** to display the list of policies.
3. Ensure the policy System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing is set to Disabled.
4. Close the Local Security Policy window.

### Application Server Role for Unified CCMP Web/Application Servers

Install the Application Server role on the servers where the Unified CCMP Web and Application Server components will be installed.

1. Click **Start > All Programs > Administrative Tools > Server Manager**. The Server Manager tool is displayed.
2. Right-click **Roles** in the left panel of the Server Manager window and then click **Add Roles**. The Add Roles Wizard displays.
3. Click **Next**.
4. Select the **Application Server** role. You will be prompted to install other dependent role features; click **Add Required Features**.
5. Click **Next**. The Introduction to Application Server information is displayed.
6. Click **Next**.
7. Add **Web Server (IIS) Support** to the selected options. You will be prompted to install other dependent features; click **Add Required Role Services**.
8. Click **Next**. The Introduction to Web Server (IIS) information is displayed.
9. Click **Next**. The role services for Web Server (IIS) information is displayed.
10. Add **IIS 6 Management Compatibility** to the selected role services.
11. Click **Next**. The Confirm Installation Selections window is displayed.
12. Click **Install**.
13. Click **Close** when the installation is complete.

The Application Server role is now configured.

### .NET Framework 3.5 Feature Installation for Unified CCMP Database Servers

For dual tier systems with a separate database server, install the .NET Framework 3.5 feature on the servers where the Unified CCMP database server components will be installed as follows:

1. Click **Start > All Programs > Administrative Tools > Server Manager**. The Server Manager tool is displayed.
2. Right-click **Features** in the left panel of the Server Manager window and then click **Add Features**. The Add Features Wizard displays.

3. Select **.NET Framework 3.5.1 Features**. You will be prompted to install other dependent features; click **Add Required Role Services**.
4. Click **Next**. The Introduction to Web Server (IIS) information is displayed.
5. Click **Next**. Web Server (IIS) Role Services are displayed.
6. Click **Next**. The Confirm Installation Selections window is displayed.
7. Click **Install**.
8. Click **Close** when installation is complete.

The .NET Framework 3.5 SP1 feature is now installed.

## Required Domain User Accounts

If setting up a dual-sided replicated Management Portal installation, you need to create domain user accounts for use by Unified CCMP. The following accounts are required:

- **sql_agent_user** This domain account is used to replicate data between Microsoft SQL Server databases. By default, Unified CCMP assumes this will be **sql_agent_user**, but you can specify a different account name during installation.

  For a single-sided installation, the Portal can create this account automatically as a local user.

  Ensure the following properties are set in the account:

  - User must change password on next login – **unchecked**
  - User cannot change password – **checked**
  - Password never expires – **checked**
  - Account is disabled – **unchecked**

- **report_execution_user** This domain account is used as the Reporting Services Execution Account. It is used by Microsoft SQL Server Reporting Services to authenticate requests when establishing the database connection used for Audit reporting within Unified CCMP.

  Ensure the following properties are set in the account:

  - User must change password on next login – **unchecked**
  - User cannot change password – **checked**
  - Password never expires – **checked**
  - Account is disabled – **unchecked**

# 3. Microsoft SQL Server Setup

## Overview

Cisco Unified CCMP requires components of Microsoft SQL Server on all Unified CCMP servers. This chapter details the process to install these components and the configuration that is required for Unified CCMP.

When SQL Server installation is complete, SQL Server Service Pack 4 should be applied to all Unified CCMP servers.

## Microsoft SQL Server Component Installation

The Microsoft SQL Server installation process allows the installation of a number of different SQL components. The components that are required for Unified CCMP are:

- Database Services.
- Reporting Services.
- Workstation components, Books Online and development tools.

Depending on the type of installation being performed, different servers within the installation may be used to host different components. In a single server installation all components must be installed on the same server. In a dual-tier installation (where the database and the web/application server exist on different machines) the database server will host the following components:

- Database Services
- Workstation components, Books Online and development tools

And the web/application server will host the following components:

- Reporting Services
- Workstation components, Books Online and development tools

More information about the exact steps to be performed when installing either of these deployment models can be found in the next section.

**Note:** During the installation of SQL Server 2005 and SQL 2005 Service Pack 4 the Windows Program Compatibility Assistant may display noting that there are compatibility issues between SQL Server 2005 and Windows Server 2008. These warnings can be ignored. If the Compatibility Assistant displays, click **Run Program** to continue with the installation.

## Installing SQL Server for a Single Server Deployment

For Unified CCMP deployments where a single server is being used to host the web/application server and the database server, the installation steps for SQL Server 2005 are as follows. To configure SQL Server 2005 for a two-tier deployment model please proceed to the Installing SQL Server for a Two-Tier Deployment section.

Note that the Application Server role must be added to the server as described in Chapter 2, Installation Guidelines and Requirements, *before* installing SQL Server as it is a prerequisite for the Reporting Services component.

Before installing SQL Reporting Services, IIS must be configured to support 32-bit applications as follows:

1. Click **Start > All Programs > Accessories** and then right-click **Command prompt** and select **Run as administrator**.
2. Copy the following script and paste into the command window:

```
cscript %SystemDrive%\inetpub\AdminScripts\adsutil.vbs set w3s
vc/AppPools/Enable32bitAppOnWin64 1
```

3. Press **Enter** to execute the script.

The 32-bit version of SQL Server 2005, including Reporting Services, can now be installed.

If you are installing a dual-sided deployment the steps in this section must be carried out on both sides of the deployment.

### Installation

To install SQL Server 2005 for a Single Server Deployment:

1. Insert the installation media and run **Servers\splash.hta** if it does not automatically launch.
2. Select **Start > Install > Server components, tools, Books Online and samples**. The Software License Agreement window displays.
3. Read the terms of the license agreement.
   - Check **I accept the license terms and conditions**.
   - Click **Next**.

   The Installing Prerequisites window displays.
4. Click **Install**. Prerequisite software is then installed. After it is installed, click **Next**; a system configuration check is performed and then the Welcome to Microsoft SQL Server Installation Wizard window displays.
5. Click **Next**. The System Configuration Check window displays.
6. When the system configuration check completes successfully, click **Next**.

The Microsoft SQL Server Installation screen displays. The Registration Information window displays.

7. Enter the following information:
   - Name
   - Company
   - Product Key

   Click **Next**. The Components to Install window displays.
8. Select **SQL Server Database Services, Reporting Services** and **Workstation components, Books Online and development tools** and click **Next**; the Instance Name window displays.
9. Select **Default** instance, then click **Next**. The Service Account window displays.
10. Select **Use the built-in System account** and choose **Local System** from the drop-down list.
11. In **Start Services** ensure the **SQL Server, SQL Server Agent** and **Reporting Services** options are checked; click **Next**. The Authentication Mode window displays.
12. Select **Mixed Mode** (Windows Authentication and SQL Server Authentication), provide the sa logon password and confirm it.
13. Click **Next**. The Collation Settings window displays.
14. Select **Collation designator and sort order**, and then choose **Latin1_General** from the drop-down list.
15. Select the **Accent – sensitive** check box in the database collation settings; click **Next**. The Report Server Installation Options window displays.
16. Ensure the **Install the default configuration** option is selected and click **Next**. The Error and Usage Report Settings window displays. You have the option of choosing:
    - Error reports
    - Feature usage
    - Neither
17. After making your choice, click **Next**. The Ready to Install window displays.
18. After reviewing the components to be installed, click **Install**. The Setup Progress window displays and installation begins.
19. When the installation has completed, click **Next**. The Completing Microsoft SQL Server 2005 Setup window displays.
20. After reviewing the provided information, click **Finish**.

The SQL Server 2005 installation is now complete. You must install SQL Server 2005 Service Pack 4 before proceeding.

## SQL Server 2005 Database Server Configuration

After the SQL Server 2005 installation has completed, configure SQL Server 2005 as follows:

1. Select **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager**. The SQL Server Configuration Manager window displays.
2. Expand **SQL Native Client Configuration** and select **Client Protocols**. A list of the client protocols displays to the right. The correct order and states are:
   - Shared Memory – Order 1; **Enabled**
   - Named Pipes – Order 2; **Enabled**
   - TCP/IP – Order 3; **Enabled**
   - VIA – **Disabled**

   If the order displayed is not as indicated above, right-click **Client Protocols** and select **Properties**. The Client Protocol Properties window displays. Use the window controls to ensure that the client protocols are in the correct order positions as described above. Click **OK** to close the Client Protocol Properties window.

   To change the Enabled status of a protocol, double-click on the protocol name and change the state in the Protocol Properties window.
3. Expand the **SQL Server Network Configuration** and select **Protocols for MS SQL Server**.
4. Ensure that **Shared Memory**, **Named Pipes** and **TCP/IP** have a status of **Enabled**; if not, right-click the disabled protocol and select Enable.
5. Ensure that the VIA protocol has a status of **Disabled**.
6. Select **File > Exit**. The SQL Server Configuration Manager closes.

SQL Server 2005 Database configuration is now complete.

## SQL Server 2005 Reporting Services Configuration

Configure SQL Server Reporting Services for a single server Unified CCMP deployment as follows.

### Granting the Network Service Account Access to Reporting Services

The Network Service account for the local server and the opposite side server, if present, must be given permission to access the Reporting Services instance:

1. Navigate using Internet Explorer to the following URL: **http://localhost/reports**.

   The Reporting Services Report Manager screen displays.
2. Select **Properties** tab. The Properties tab displays with the Security section open.
3. Select **New Role Assignment**. The New Role Assignment window displays.

4. Add the Network Service account for this server (NT AUTHORITY\NETWORK SERVICE) in Group or user name.
5. Select the following Roles from the list:
   - Browser
   - Content Manager
   - My Reports
   - Publisher
   - Report Builder

   Click **OK** to add the new role assignment. The Security section of the Properties tab displays, showing the new user role assignment.
6. If more than one server exists in this installation, repeat steps 2 to 5 setting the other side's Network Service account in place of the standard NT Authority\Network Service entry used in step 4. Enter the name of the machine in the `<DOMAIN>\<MACHINENAME$>` form. So for the machine called CCMPSIDEB on the CISCO domain enter `CISCO\CCMPSIDEB$`.
7. Select the **Site Settings** link at the top of the page. The Site Settings window displays.
8. Select the **Configure site-wide security** link. The System Role Assignments window displays.
9. Select **New Role Assignment**. The New Role Assignment window displays.
10. Add the Network Service account for this server (NT AUTHORITY\NETWORK SERVICE) in Group or user name.
11. Choose the following Roles from the list:
    - System Administrator
    - System User

    Click **OK** to add the new role assignment. The System Role Assignments window displays.
12. If more than one server exists in this installation then repeat steps 9 to 11 setting the other side's Network Service account in place of the standard NT Authority\Network Service entry used in step 10. Enter the name of the machine in the `<DOMAIN>\<MACHINENAME$>` form. So for the machine called CCMPSIDEB on the CISCO domain enter `CISCO\CCMPSIDEB$`.

### Reporting Services Execution Account Setup

The Reporting Services Execution Account is used is used by Microsoft SQL Server Reporting Services to authenticate requests when establishing the database connection used for audit reporting in Unified CCMP. See Required Domain User Accounts in Chapter 2 for further details on creating the Reporting Services Execution Account user account.

1. Select **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > Reporting Services Configuration Manager**. The Reporting Services Configuration Manager displays.

2. Select **Execution Account** option from the list on the left of the window. Check the box for **Specify an execution account** and enter the domain account information for the execution account.
3. Click **Apply**.
4. Click **Exit** to close the Reporting Services Configuration Manager.

SQL Server 2005 installation and configuration for a single tier deployment is now complete.

## Installing SQL Server for a Two-Tier Deployment

For Unified CCMP deployments where a the web/application server components and the database components will reside on separate servers, the installation steps for SQL Server 2005 are as follows.

If you are installing a dual-sided deployment the steps in this section must be carried out on both sides of the deployment.

**Note:** The database server ***must*** be installed before the web server.

### Database Server: SQL Server Installation

Install SQL Server on the database servers first. The database servers will host the SQL Server database and workstation components.

The steps to install Microsoft SQL Server 2005 on the database servers are as follows:

1. Insert the installation media and run **Servers\splash.hta** if it does not automatically launch.
2. Select **Start > Install > Server components, tools, Books Online and samples**. The Software License Agreement window displays.
3. Read the terms of the license agreement.
   - Check **I accept the license terms and conditions**.
   - Click **Next**.

   The Installing Prerequisites window displays.
4. Click **Install**. Prerequisite software is then installed. After it is installed click **Next**; a system configuration check is performed and then the Welcome to Microsoft SQL Server Installation Wizard window displays.
5. Click **Next**. The System Configuration Check window displays.
6. When the system configuration check completes successfully, click **Next**.

**Note:** Warnings may be displayed stating that IIS has not been installed and ASP.Net Version Registration Requirements have not been met. These warnings can be ignored as these components are not required for the database server in a two-tier deployment.

The Microsoft SQL Server Installation window displays.

The Registration Information window displays.

7. Enter the following information:
   - Name
   - Company
   - Product Key

   Click **Next**. The Components to Install window displays.
8. Select **SQL Server Database Services and Workstation components, Books Online and development tools**; click **Next**. The Instance Name window displays.
9. Select **Default** instance, and then click **Next**. The Service Account window displays.
10. Select **Use the built-in System account** option, and then select **Local System** from the drop-down list.
11. In **Start services at the end of setup** section ensure SQL Server and SQL Server Agent options are checked, click **Next**. The Authentication Mode window displays.
12. Select **Mixed Mode** (Windows Authentication and SQL Server Authentication), provide the sa logon password and confirm it.
13. Click **Next**. The Collation Settings window displays.
14. Select **Collation designator and sort order**, choose **Latin1_General** from the drop-down list.
15. Select **Accent – sensitive** check box in the database collation settings, click **Next**. The Error and Usage Report Settings screen displays. You have the option of choosing:
    - Error reports
    - And/or feature usage
    - Neither
16. Make your choice, and then click **Next**. The Ready to Install window displays.
17. After reviewing the components to be installed, click **Install**. The Setup Progress screen displays and installation begins.
18. When the installation has completed, click **Next**. The Completing Microsoft SQL Server 2005 Setup window displays.
19. After reviewing the provided information, click **Finish**.

Installation of the SQL Server 2005 database component is complete. You must now install SQL Server 2005 Service Pack 4 before proceeding.

## Database Server: SQL Server Configuration

After the SQL Server 2005 database component installation has completed, configure SQL Server 2005 as follows:

1. Select **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager**. The SQL Server Configuration Manager displays.
2. Expand **SQL Native Client Configuration** and select **Client Protocols**. A list of the client protocols displays to the right. The correct order and states are:
   - Shared Memory – Order 1; **Enabled**
   - Named Pipes – Order 2; **Enabled**
   - TCP/IP – Order 3; **Enabled**
   - VIA – **Disabled**

   If the order displayed is not as indicated above, right-click **Client Protocols** and select **Properties**. The Client Protocol Properties window displays. Use the window controls to ensure that the client protocols are in the correct order positions as described above. Click **OK** to close the Client Protocol Properties window.

   To change the Enabled status of a protocol, double-click on the protocol name and change the state in the Protocol Properties window.
3. Expand **SQL Server 2005 Network Configuration** and select **Protocols** for MS SQL Server.
4. Ensure that **Shared Memory, Named Pipes** and **TCP/IP** have a status of **Enabled**. If not, right-click the Disabled protocol and select Enabled.
5. Ensure that **VIA** protocol is in the **Disabled** state.
6. In Menu select **File > Exit**. The SQL Server Configuration Manager closes.

Installation and configuration of SQL Server components on the database server is now complete.

## Configuring Windows 2008 R2 Firewall for SQL Server

**Note:** By default the Windows Server 2008 R2 Firewall will not allow incoming traffic for SQL Server. If the Windows firewall is on create a rule to allow SQL Server traffic as follows:

1. Click **Start** > **All Programs > Administrative Tools > Server Manager**.
2. Expand the **Configuration** item in the left hand panel.
3. Expand **Windows Firewall with Advanced Security** and click on **Inbound Rules**. A list of firewall rules is displayed.
4. Click **New Rule** in the Actions panel. The **New Inbound Rule Wizard** is displayed.
5. Select **Port** as the rule type and click **Next**.
6. Select **TCP** as the protocol and enter **1433** as the specific local port.
7. Click **Next**. The Action options are displayed.
8. Choose **Allow the connection**.
9. Click **Next**. The Profile options are displayed.

10. Select the profile options that are appropriate to your deployment and click **Next**.
11. Enter a name for the rule and click **Finish** to create the rule.

The new rule will appear in the list of inbound rules as an enabled rule.

## Web Server: SQL Server Installation

The Unified CCMP web servers must have Microsoft SQL Server Reporting Services and the Workstation Components installed. The Reporting Services component of Microsoft SQL Server is installed as part of the standard SQL Server installation process.

**Note:** The Application Server role must be added to the web servers as described in Chapter 2, Installation Guidelines and Requirements, *before* installing SQL Server Reporting Services as it is a prerequisite for the installation.

Before installing SQL Reporting Services, IIS must be configured to support 32-bit applications as follows:

1. Click **Start > All Programs > Accessories** and then right-click **Command prompt** and select **Run as administrator**.
2. Copy the following script and paste into the command window:

   ```
   cscript %SystemDrive%\inetpub\AdminScripts\adsutil.vbs set w3s
   vc/AppPools/Enable32bitAppOnWin64 1
   ```

3. Press **Enter** to execute the script.

The 32-bit version of SQL Server 2005 Reporting Services can now be installed.

The steps to install Microsoft SQL Reporting Services on the Web Server are as follows:

1. Insert the installation media and run **Servers\splash.hta** if it does not automatically launch.
2. Select **Start > Install > Server components, tools, Books Online and samples**. The Software License Agreement window displays.
3. Read the terms of the license agreement.
   - Check **I accept the license terms and conditions**.
   - Click **Next**.

   The Installing Prerequisites window displays.
4. Click **Install**. The Welcome to Microsoft SQL Server Installation Wizard window displays.
5. Click **Next**. The System Configuration Check window displays.

6. When the system configuration check completes successfully, click **Next**. The Microsoft SQL Server Installation, then the Registration Information window displays.
7. Enter the following information:
    - Name
    - Company
    - Product Key fields

    Click **Next**. The Components to Install window displays.
8. Select **Reporting Services, Workstation components, Books Online and development tools**, and then click **Next**. The Instance Name screen displays.
9. Select **Default** instance, and then click **Next**. The Service Account window displays.
10. Select **Use the built-in System account** and select **Local System** from the drop-down list.
11. In **Start** services ensure **Reporting Services** is checked; click **Next**. The Report Server Installation Options window displays.
12. The options for configuring the Report Server Instance will be disabled because the SQL Database Services are not installed on this machine. Ensure that the **Install but do not configure the server** option is selected and click **Next**. The Error and Usage Report Settings window displays. Select from:
    - Error reports
    - And/or feature usage
    - Neither
13. Make your choice, and then click **Next**. The Ready to Install window displays.
14. After reviewing the components to be installed, click **Install**. The Setup Progress window displays and installation begins.
15. When the installation has completed, click **Next**. The Completing Microsoft SQL Server 2005 Setup window displays.
16. Review the information, and then click **Finish**.

Installation of the SQL Server 2005 Reporting Services component is now complete. You must now install SQL Server 2005 Service Pack 4 before proceeding.

## Web Server: SQL Server Configuration

Following the installation of the SQL Server 2005 Reporting Services component, the SQL Server Reporting Services instance must be configured and appropriate access permissions must be granted on each Reporting Services instance for the local Network Service account and for the Network Service account of all other web servers in the Unified CCMP deployment.

### Reporting Services Configuration

Configure Reporting Services as follows:

1. Select **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > Reporting Services Configuration**. The Reporting Services Configuration Manager displays.
2. Click **Connect** to select the Report Server instance that has just been installed and load its configuration. The Reporting Services Configuration Manager loads the instance configuration information.
3. Configure the Report Server Virtual Directory:
    a. In the left panel select **Report Server Virtual Directory**. The Report Server Virtual Directory Settings window displays.
    b. Click **New**, the Create a New Virtual Directory window displays with the default Virtual Directory name of ReportServer. Click **OK**. The ReportServer virtual directory is created.
4. Configure the Report Manager Virtual Directory:
    a. In the left panel select **Report Manager Virtual Directory**. The Report Manager Virtual Directory Settings window displays.
    b. Click **New**, the Create a New Virtual Directory window displays with the default Virtual Directory name of Reports. Click **OK.** The Reports virtual directory is created.
5. Configure the Web Service Identity:
    a. In the left panel select **Web Service Identity**. The Web Service Identity window displays.
    b. Click **New** next to Report Server to create a new application pool for the Report Server.
    c. Enter a name, such as ReportServer, for the application pool.
    d. Select **Built In Account**.
    e. Select **Local System.**
    f. Click **OK.**
    g. Click **New** next to Report Manager to create a new application pool for the Report Manager.
    h. Enter a name, such as ReportManager, for the application pool.
    i. Select **Built In Account**.
    j. Select **Local System.**
    k. Click **OK.**
    l. Click **Apply** to configure the identity for the new virtual directories. After configuration is complete a green tick displays to confirm that the identity has been set correctly.
6. Setup the ReportServer database:
    a. In the left panel select **Database Setup**. The Database Connection window displays.
    b. Enter the name of the database server associated with this web server in **Server Name**.

c. Click **Connect** and confirm the credentials that will be used to access the database. These credentials will be used to connect to the database server and create the ReportServer database.

d. Click **New** next to Database Name field. The SQL Server Connection dialog box displays.

e. Enter **ReportServer** in the **Database Name** field. Specify a valid user account to connect to the database server. This may be Current User – Integrated Security if using a domain user that has administrator access to the SQL Server instance on the database server because these credentials will be used to connect to the database server and create the ReportServer database.

f. Click **OK**. After a short pause the SQL Server Connection window closes and you will be returned to the Database Connection window and the Report Server database creation will execute.

g. When the Task Status pane indicates that the ReportServer database creation process has completed, click **Apply** to associate the new database to the report server. The SQL Server Connection dialog box displays.

h. Specify a valid user account to connect to the database server. This may be Current User – Integrated Security if using a domain user that has administrator access to the SQL Server instance on the database server. Click **OK**.

After a short pause the action will complete and a series of green ticks display to confirm that the database has been added.

7. Configure the Reporting Services Execution Account:

   a. Click the **Execution Account** option from the list on the left of the window. Check the box for **Specify an execution account** and enter the domain account information for the execution account. The Reporting Services Execution Account is used is used by Microsoft SQL Server Reporting Services to authenticate requests when establishing the database connection used for audit reporting in Unified CCMP. See Required Domain User Accounts in Chapter 2 for further details on creating the Reporting Services Execution Account user account.

   b. Click **Apply**.

8. Click **Exit** to close the Reporting Services Configuration Manager.

### Granting the Network Service Account Access to Reporting Services

The Network Service account for the local web server and all other web servers in the Unified CCMP deployment must be given permission to access the Reporting Services instance:

1. On the web server, navigate using Internet Explorer to the following URL: **http://localhost/reports**.

   The Reporting Services Report Manager screen displays.

2. Select **Properties** tab. The Properties tab displays with the Security section open.
3. Select **New Role Assignment**. The New Role Assignment window displays.
4. Add the Network Service account for this server (NT AUTHORITY\NETWORK SERVICE) in Group or user name.
5. Select the following Roles from the list:
   - Browser
   - Content Manager
   - My Reports
   - Publisher
   - Report Builder

   Click **OK** to add the new role assignment. The Security section of the Properties tab displays, showing the new user role assignment.
6. If more than one web server exists in this installation, repeat steps 2 to 5 setting the other side's Network Service account in place of the standard NT Authority\Network Service entry used in step 4. Enter the name of the machine in the `<DOMAIN>\<MACHINENAME$>` form. So for the machine called CCMPSIDEB on the CISCO domain enter `CISCO\CCMPSIDEB$`.
7. Select **Site Settings** link at the top of the page. The Site Settings window displays.
8. Select the **Configure site-wide security** link. The System Role Assignments window displays.
9. Select **New Role Assignment**. The New Role Assignment window displays.
10. Add the Network Service account for this server (NT AUTHORITY\NETWORK SERVICE) in Group or user name.
11. Choose the following Roles from the list:
    - System Administrator
    - System User

    Click **OK** to add the new role assignment. The System Role Assignments window displays.
12. If more than one server exists in this installation then repeat steps 9 to 11 setting the other side's Network Service account in place of the standard NT Authority\Network Service entry used in step 10. Enter the name of the machine in the `<DOMAIN>\<MACHINENAME$>` form. So for the machine called CCMPSIDEB on the CISCO domain enter `CISCO\CCMPSIDEB$`.

The installation and configuration of SQL Server 2005 for Unified CCMP is now complete.

# 4. Component Installation

This chapter describes the procedure for installation of the individual CCMP software components.

For a description of the layout of the software components for different deployment models please see the section Unified CCMP Architecture in Chapter 1.

## Planning Your Installation

Components should be installed in the order described in this document.

For dual-sided, or replicated, systems, perform a complete installation on the Side A servers followed by a complete installation on the Side B servers. After this is completed, you can perform the Unified CCMP configuration (including replication), as detailed in Chapter 5, Component Configuration.

To assist with troubleshooting installation issues it is possible to install Unified CCMP components with logging enabled. This process is described in Chapter 9, Troubleshooting.

## Recording Your Settings

During the installation procedure you will need to record information that will be required for future reference. Use the table below to record this information and store it in a secure location when the installation is complete.

| **Management Portal** | |
|---|---|
| Database Catalog Name | |
| sql_agent_user Password | |
| Cryptographical Passphrase | |
| Administrator Password | |
| **ICM** | |
| Application Name | |
| Application Key | |
| Local Registry Port | |
| **Network Applications Manager (NAM) (if present)** | |
| Application Name | |
| Application Key | |
| Local Registry Port | |

**Note: The cryptographical passphrase is a vital piece of information and must be recorded.** It is used for encrypting and decrypting system passwords. It is selected during the initial installation of the database component and is used during the

installation of the other components and in any future installations, such as adding new servers to the Unified CCMP cluster, or upgrading the software.

# Component Installation

## Component Installation using the Unified CCMP CD

The installation for a component must take place on the server on which the component is being installed. Remote installation of components is not available.

1. Insert the Unified CCMP CD. A window consisting of a main panel and a number of tabs, corresponding to the Management Portal components, displays.
2. **Note:** If autorun is disabled and you have not been presented with Unified CCMP Products Installation Application, double-click the **autorun.bat** file to launch Unified CCMP installer.

   **Note:** If Windows User Access Control (UAC) is enabled then setup should be launched by right-clicking the **autorun.bat** file and selecting the **run as administrator** option.
3. Clicking on a component in the left hand panel displays the list of prerequisites for that component and allows you run a test to check that those prerequisites are installed.
4. To begin the installation of each individual component, click its tab. Then click the **Run Test** button to check that the listed prerequisite applications are installed. When the installer has verified the presence of these components, the **Install** button is enabled, allowing you to proceed with the installation of that component.

   **Note:** A red cross appears next to any prerequisite application that is not installed. This indicates that the application must be installed before the installation of the selected component can proceed. After all the prerequisite software is installed click **Re-Run Test** to enable the **Install** button.
5. When all the prerequisite applications display a green tick next to them, click **Install** to install the chosen component.

# Database Component

This section details how to install Unified CCMP Database server components. The Database Install Tool component is installed and is then used to set up the Unified CCMP database.

## Database Install Tool Installation

To install Unified CCMP Database component, perform the following steps.

**Note:** This does not install a new database component. It installs the Database Installation tool, which is then used to set up the database.

1. Select the **Database Component** tab; click **Run Test** to check for prerequisites, and click **Install**. Click **Next** to go through each window in turn.
2. 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. Read it thoroughly before accepting.
3. In the **Cryptography Configuration** window:

   **Passphrase** Create a cryptographical pass phrase 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 cluster.

   **Confirm Passphrase** You cannot continue until the contents of this field are identical to the passphrase entered above.

   **Caution** The cryptographical passphrase is a vital piece of information and must be recorded for use when installing later components and when adding or replacing servers in the future.

   **Caution** If you are upgrading a previous version of the Unified CCMP or adding a new server to an existing cluster, you must use the same cryptographical passphrase as was originally used. If you do not know the original passphrase, immediately cease installation and call your support provider. If you continue installation with a new passphrase, you will be unable to access your existing data.
4. In the **Destination Folder** window, review the location. If necessary, click **Change** to change the location where you want the Database Server component to be installed.
5. Click **Install.**

   To set up your database now, ensure that the **Launch Management Portal: Database Install Tool** check box is checked before clicking **Finish**.

The installation of the Database Install Tool is now complete.

## Database Setup

If you checked the **Launch Management Portal: Database Install Tool** check box after installing the Database component, the database install tool launches automatically. You can also launch the database install tool manually from **Start > All Programs > Management Portal > Database > Database Installer.**

The wizard will guide you through the process of installing a database.

Click **Next** to go through each window in turn. Enter the following details:

1. In the SQL Server Connection Details window:
    - **Server Name** Select the Microsoft SQL Server where the Unified CCMP database will be installed. In most cases this will be the machine running the Install Tool application, in which case it must be left as the default **(local).**
    - **Database Name** Enter or select the name of the database catalog that will be used for Unified CCMP. Use the default name of **Portal.**
    - **Connect Using** Select the radio button of the login credentials you want to apply:
        - 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** Make sure the connection to the Microsoft SQL Server is established. The message "Connection succeeded but database does not exist" appears at this point. Click **OK** to continue.
2. In the **Select an Action to Perform** window select **Install a New Database**.
3. In the **Setup Replication** window:
    - **Replicated Configuration** Replication only needs to be configured on Side B of a dual-sided system. Check this box if this database installation is on Side B of a dual-sided, replicated system.
    - **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 Microsoft SQL Server. By default, it is **C:\Program Files (x86)\Microsoft SQL Server\MSSQL.1\MSSQL\repldata.**
4. The fields on the **Configure the Location of Data Files** window only need to be amended if you want to customize the size and location of the database files, otherwise click **Next.**
    - **Location** When you select a File Group, its location is shown in this field. To change this location, browse to the new location.
    - **Initial Size** Select the space that must be allocated for this File Group. The default is based on the Portal's analysis of your system.

- **Max Size** Set the storage capacity for the selected File Group. You can also choose to set no limit to the file size by selecting the **Unrestricted Size** check box, although this is not recommended.
- **Update** Saves your changes to the selected File Group.
- **Default** Returns the settings for all File Groups to their default.

5. The **Configure SQL Server Agent Service Identity** window sets up a user account that is used by Microsoft 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 user account. This defaults to **sql_agent_user**. If you used a different name when setting up the account, enter that name instead.
   - **Automatically create the user account if missing** For a single-sided system, it is possible to create the required user automatically. *For all other systems, you must set up the required account manually*. If you have not already created the user account, set it up now before continuing.
   - **Password** Enter a password for the user.
   - **Confirm Password** You are unable to continue until the contents of this field are identical to the passphrase entered above.
6. In the **Web Application Servers Network Service Configuration** window, enter the details of each Web Server, from both sides, to be used in the installation:
   - **Domain** The network domain the web server resides; for example, UCCMPDOM.
   - **Machine Name** The name of the machine; for example, WEBSERVERA.

     **Note:** The database installer will use this information to grant access for the Network Service accounts on these web servers to the Portal database. If you need to add a new Web Server after the database has been installed you will need to grant permissions manually. For information on how to add these permissions manually, refer to Chapter 9, Troubleshooting, for details.
7. Click **Add** to add each Web Server to the list.
8. When all Web Servers in the deployment have been added, click **Next** to begin the database setup. Setup will take several minutes.
9. When setup completes click **Close** to close the installer.

Unified CCMP database setup is now complete. For dual-sided replicated systems, repeat the database installation on the Side B database server. Replication of the databases is performed as part of the Component Configuration process described in Chapter 4, Component Configuration.

### Granting the Reporting Services Execution Account Permissions on the Unified CCMP Database

When installing a two-tier Unified CCMP deployment, permissions must be granted on the Unified CCMP database for the Reporting Services execution account. This is achieved by performing the following steps on all database servers after Unified CCMP Database Installation has been completed:

1. Select **Start > All Programs > Microsoft SQL Server 2005 > SQL Server Management Studio**. The SQL Server Management Studio displays.
2. Enter the credentials of the database server and click **Connect**.
3. Expand **Security > Logins** folder. Right-click **Logins** folder and select **New Login**. The Login – New window displays.
4. Enter the login name of the reporting execution account user. This will be in the `<DOMAIN>\<Username>` form.
5. Select **User Mapping** option in the left of the window. The User Mapping information for the execution user displays.
6. The following configuration must be applied in this window:
   - Check the check box in the **Map** column next to the **Portal** database.
   - While the Portal database is selected check the following check boxes in the **Database role membership for: Portal** section of the screen:
     - portalapp_role
     - portalreporting_role
     - portalrs_role

   Click **OK** to save the new permissions and then click **Close**.

## Application Server Component

This section details how to install and configure Unified CCMP Application Server component. The application server must be installed on all web servers in the Unified CCMP deployment.

### Application Server Component Installation

To install the Unified CCMP Application Server component, select the Application Server Component tab, click **Run Test** to check for prerequisites, and click **Install.**

Click **Next** to go through each window in turn.

1. 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. Read it thoroughly before accepting.
2. In the **Destination Folder** window, accept the folder or click **Change** to change the location for the Application Server component.
3. In the **Cryptography Configuration** window:

- **Passphrase** Enter the Cryptographical Passphrase chosen when installing the Database component.
- **Confirm Passphrase** You are unable to continue until the contents of this field are identical to the passphrase entered above.

  **Caution** The cryptographical passphrase is a vital piece of information and must be recorded for use when adding or replacing servers in the future. If you are upgrading a previous version of the Management Portal or adding a new server to an existing cluster, you must use the same cryptographical passphrase as was originally used. If you do not know the original passphrase, immediately cease the installation and call your Support Provider. If you continue installation with a new passphrase, you will be unable to access your existing data.

4. In the Cluster Configuration Database Connection window:
   - **SQL Server** Enter the name of the server where the Portal database has been installed.

     **Note:** The default value of the local machine is valid only for a standalone system. For a dual-sided system enter the name of the database server associated from the same side of the deployment.
   - **Catalog Name** Enter the name of the database, as selected in the Database Component installation. By default this is **Portal**.
   - It is recommended that you **Connect Using Windows authentication**. If the database server is on a different network, select **Microsoft SQL Server authentication** and enter the appropriate Login ID and Password in the fields provided.
5. Click **Install**. During the installation, command windows display while the installer configures Reporting Services. These command windows close by themselves and require no action from you.
6. When the installation has completed, click **Finish.**

The application server installation is now complete.

# Web Server Component

This section details how to install and configure the Unified CCMP Web Server component. The web server must be installed on all web servers in the Unified CCMP deployment.

## Web Server Component Installation

To install the Unified CCMP Web Server component, select the Web Server Component tab, click **Run Test** to check for prerequisites and click **Install.**

Go through each step in turn.

1. 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 must read it thoroughly before accepting.

2. Click **Install.** During the installation, command windows may display while the installer configures Microsoft IIS. These command windows close by themselves and require no action from you.
3. When the installation is completed, click **Finish.**

Installation of the web server component is now complete.

# Data Import Server Component

## Data Import Server Component Installation

Install the Data Import Server component on the Database servers.

To install the Unified CCMP Data Import Server component, select the Data Import Server Component tab, click **Run Test…** to check for prerequisites, and click **Install.**

Click **Next** to go through each window in turn. You will need to enter the following details:

1. 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. Read it thoroughly before accepting.
2. In the Cryptography Configuration window:
   - **Passphrase** Enter the cryptographical passphrase you created during installation of the Database Server component.
   - **Confirm Passphrase** You are unable to continue until the contents of this field are identical to the passphrase entered above.
3. In the Configure Database window:
   - **SQL Server** Accept the default value of localhost as the server on which the database resides.
   - **Catalog Name** Enter the name of the database as defined during the installation of the Database Component. The default is **Portal**.
   - Select **Connect Using Windows authentication**. Microsoft SQL Server authentication is used only when connecting to a database server on a different network, which is not supported in this release.
4. Select either **Complete** or **Custom** setup type. **Custom** setup allows the Data Import Server components to be installed to different destination folders. Use **Complete** setup to maintain all the components in a common destination folder, this is the recommended option.
5. In the **Destination Folder** window, click **Change** to change the location where the Data Import Server component installs. It is not necessary to install all Portal components to the same location.
6. In the **Session File Folder** window, click **Change** to change the location in which temporary importer files are stored. The default directory for these is based on the destination folder specified in the previous step.
7. Click **Install.**
8. When the installation is completed, click **Finish.**

9. Close the installer window.

Installation of the Data Import Server component is now complete.

# Provisioning Server Component

## Provisioning Server Component Installation

The Provisioning Server component must be installed on the servers hosting the Database Component.

To install the Unified CCMP Provisioning component, select the Provisioning Server Component tab, click **Run Test** to check for prerequisites, and click **Install.**

Click **Next** to go through each window in turn.

1. 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. Read it thoroughly before accepting.
2. In the Cryptography Configuration window:
   - **Passphrase** Enter the cryptographical passphrase you created during installation of the database component.
   - **Confirm Passphrase** Reenter the passphrase.
3. In the Configure Database window:
   - **SQL Server** Accept the default of (local) for the current machine.
   - **Catalog Name** The name of the Unified CCMP database. By default this is **Portal**.
   - **Connect Using** Select the radio button of the login credentials you want to apply:
     - **Windows authentication**.
     - **SQL Server authentication** Only select this option if you are using a database catalog on a different domain. For this option you must enter your Microsoft SQL Server Login Name and Password in the fields provided.
4. In the Destination Folder window, click **Change** to change the location where the Provisioning Server component is installed. It is not necessary to install all Unified CCMP components to the same location.
5. Click **Install.**
6. When the installation is completed, click **Finish**.

Installation of the Provisioning Server component is now complete.

# Diagnostic Framework

## Diagnostic Framework Installation

In this release, the Diagnostic Framework must be installed on all Unified CCMP servers.

To install the Diagnostic Framework, select the Diagnostic Framework, click **Run Test** to check for prerequisites, and click **Install.**

Click **Next** to go through each window in turn.

1. 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. Read it thoroughly before accepting.
2. In the **Destination Drive** window, click **Change** to change the drive location that the Diagnostic Framework is installed to.
3. In the **Select Certificate** window, you can select the type of certificate installed with the diagnostic framework.
    - **Self-Signed Certificate –** 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.
4. Click **Install.**
5. When the installation is completed, click **Finish.**

Installation of the Diagnostic Framework component is now complete.

When all Unified CCMP components are installed on the target servers, proceed to Chapter 5, Component Configuration, to configure the Unified CCMP cluster.

# 5. Component Configuration

This chapter describes how to use the Configuration Manager tool to provide information to Unified CCMP about the servers that exist in your deployment. This includes the Unified CCMP servers themselves as well as the servers that Unified CCMP will connect to such as Unified CCE and Unified CM servers.

After the configuration information is supplied, the components of Unified CCMP will be able to communicate with one another to perform such activities as importing Unified CCE configuration items.

This chapter also covers the setup of data replication for dual-sided systems. Before replication can occur, the servers in the cluster must first be set up with the required prerequisite software and Unified CCMP components.

## Unified CCMP Cluster Configuration Overview

This section describes the process for configuration of the Unified CCMP server cluster, configuration of Unified CCE to allow Unified CCMP to connect, and setup of data replication in a dual-sided Unified CCMP system.

The Unified CCMP Configuration Manager is an application that is used to configure server clusters. A Unified CCMP cluster consists of the Unified CCMP servers as well as the Cisco Unified CCE servers and Unified CM servers that Unified CCMP connects to.

Before beginning cluster configuration, you must:

- Configure **AWDB database security** to allow Unified CCMP to connect.
- Set up the **common ConAPI credentials** and the **CMS server** on the Unified CCE environments.

You will then configure the server cluster using the Configuration Manager. You need to input the list of servers and the configuration data for each in the following order:

- **Portal Servers** – the details of the servers containing Unified CCMP components. For dual-sided systems, replication is configured at this point.
- **Unified CCE** – the details of the servers hosting Unified CCE and the database credentials for accessing their data.
- **Unified CM** – the details of the servers hosting the Unified CM, the endpoint and security credentials for accessing the AXL interface.
- **Network Applications Manager** (only relevant for hosted deployments of Unified CCE) – the details of the servers hosting NAM's and the database credentials for accessing their data.

**Note:** In a dual-sided Unified CCMP environment, you only need to run the Unified CCMP Configuration Manager application on the **Side A Database server.**

## AWDB Database Security Configuration

The AWDB database must be configured to allow Unified CCMP to connect.

**Note:** No configuration of the AWDB is required if Unified CCMP uses SQL Server Authentication to connect to the ICM and there is an appropriate SQL user that can be used to read data on the AW. However, the SQL login used for the connection must have the appropriate permissions on the AWDB (see below).

If configuration is required do the following:

1. Log in to the AWDB as a domain user with local administrative privileges.
2. Click **Start > All Programs > Microsoft SQL Server > Management Studio** connect to the server.
3. Open the **Security** folder and right-click on **Logins**.
4. Select **New Logins** from the drop-down list. The Login – New window displays.
5. Add SQL logins for each server hosting the Data Import Server in this installation by completing the fields as follows:
   - General page
     a. **Login Name** enter the name for the machine in the `<DOMAIN>\<MACHINENAME>$` form. This configures access for the NETWORK SERVICE account from the Web Application Server machine.
     b. **Authentication** Select **Windows Authentication** unless connecting to a server on a different domain.
     c. Click **OK**.
   - User Mapping page
     a. **Users mapped to this login** Check the check box for the AWDB
     b. **Database role membership for: AWDB** grant the following roles to the login by checking the corresponding check boxes:
        - Public
        - db_datareader
     c. Click **OK**.

AWDB Security configuration is now complete.

## Common ConAPI Credentials

For each Unified CCE, you must set up an application instance to connect through **ConAPI**. This is used by Unified CCMP when making provisioning requests to add, update, or delete items. You can use an existing application instance or create a new one.

If you are using a Cisco Unified Interaction Manager installation integrated with Unified CCE, the Portal can be set up to use the application instance that was configured for the Cisco Unified Interaction Manager deployment. This enables you to provision non-voice skill groups and other items through Unified CCMP. To do

this, leave the **Application type** for the application instance as **Other** but change the **Permission level** to **Full read/write**. Information on configuring the application instance for a Cisco Unified Interaction Manager deployment can be found in the *Cisco Unified Web and E-Mail Interaction Manager Deployment and Maintenance Guide*.

To create an application instance, run the Configuration Manager on the Unified CCE administration workstation server as follows:

1. Open the Configuration Manager. This can normally be done from **Start > Program Files > Administration & Data Server > Configuration Manager**.

   **Note:** If you are connecting to the Unified ICM server using Remote Desktop, you need to set the **/console** switch in order to run the Configuration Manager.

2. Under **Tools/List Tools** double-click **Application Instance List** to open it.
3. Click **Retrieve** to display the list of configured application instances. 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 the Portal to connect. This must 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** to save the new application instance**.**

Creation of an application instance is now complete.

## CMS Server Setup

Before configuring the Unified CCMP server cluster, you must ensure that the CMS Server's are set up correctly on each Unified ICM/Network Applications Manager (NAM) AW.

**Note:** Each Unified ICM requires a separate Administration & Data Server running a single instance of CMS server.

Check that when the Administration & Data Server was configured, the **CMS Node** option was selected. You can determine if this was the case by looking for a **cmsnode** and a **cms_jserver** process running on the Unified ICM.

If these processes are not present, you must set the **CMS Node** option on the Unified ICM. See the appropriate documentation for details on how to do this.

A new application connection must be defined on each configured Unified ICM for each Provisioning Server that will connect to it. This ensures that in a dual-sided system, the alternate side can also connect to the Unified ICM in a failover scenario. To do this:

1. Select **Start > Run > C:\icm\bin\cmscontrol.exe** in the Unified ICM being configured. This opens the CMS control console.
2. Click **Add** to the right of the window to launch the **Application Connection Details** window and fill in the fields as follows:
   - **Administration & Data Server link** Use the machine name of the Unified CCMP Database Server, in capital letters, with 'Server' appended, such as UCCMPServer
   - **Administration & Data Server RMI registry port** This is the port on the CICM for the Unified CCMP Provisioning server to connect to. This will usually be 2099; however if the Unified CCMP Provisioning Server is connecting to multiple Unified ICMs, or the Unified ICMs are configured as dual-sided, then a different port must be allocated for each Administration & Data Server.
   - **Application link** Use the machine name of the Unified CCMP Database Server, all in capital letters, with 'Client' appended, such as UCCMPDBClient.
   - **Application RMI registry port** This is the port on the Unified CCMP Database Server for the Unified ICM to connect to the Provisioning Server. For convenience, this must be configured the same as for the Administration & Data Server RMI registry port.

     **Note:** Each Unified ICM that the Portal will be provisioning must use a unique port. For example if Unified CCMP is configured to provision two dual-sided Unified ICMs then each Unified ICM must be assigned a unique port number. This port number must be configured in the Administration & Data Server RMI registry port and in the Application RMI registry port. It will also be used later when the ConAPI connection is configured in the Unified CCMP Configuration Manager.
   - **Application host name** The Unified CCMP Database Server name or fixed IP address, such as UCCMPDB or 240.24.53.107.
3. Click **OK** twice to save your changes and close the CMS control console.

For a dual-sided Unified CCMP system two entries are required in the CMS control utility on each separate Administration & Data Server. These entries will refer to the side-A Unified CCMP Provisioning Server and the side-B Unified CCMP Provisioning Server.

## Unified CCMP Configuration Procedure

After the Unified CCE application instances and CMS Server configuration is complete the Unified CCMP server cluster proceed as follows. Perform these steps on the server where the Unified CCMP database component is installed. For a dual-sided system perform these steps on the Side A database server.

1. Click **Start > All Programs > Management Portal > Configuration Manager**.
2. The **Database Connection** window displays. On this window:
   - **Server Name** This option defaults to the current machine and cannot be changed.

- **Database** Select the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal.**
- **Authentication** To connect to the Portal database using the credentials of the currently logged-in user select **Windows Authentication** (this is the recommended option). To connect using SQL Server Authentication, select **SQL Server Authentication** and enter the name and password of a SQL user with write access to the Portal database.

3. Click **OK** to open the Configuration Manager.
4. Enter the settings as described in the following sections.
5. When complete, click **Save** to save your settings, or **Revert** to cancel your changes.

**Note:** When using Windows Authentication, the user running the **Configuration Manager** application must have permission to execute SQL commands on the Unified CCMP database.

## Physical Servers

All servers that will belong to the Unified CCMP cluster must be entered here. This includes the Unified CCMP servers themselves and the Unified CCE or Unified CM servers that will be managed by Unified CCMP. Later on in the configuration process the role of each server will be defined.

1. Click **New** to add a new server to the cluster. The **Server Configuration** window displays.

   **Note:** When this is done for the first time, the details will default to those of the current server.

   - **Server Name** Enter the name of the server, such as UCCMPA.
   - **Default Hostname** Enter the hostname of the machine. This is the unique name by which it is known on the network. The machine must be accessible using this host name from anywhere in the cluster.

   **Note:** The Default Hostname cannot be an IP address.

   - **Default IP Address** Enter the IP address of the server.
2. Click **OK.**

Repeat these steps for all Unified CCMP servers, Unified ICM Servers, Unified CM Servers and NAM Servers (hosted deployments of Unified CCE) in this installation.

## UCCMP Servers

Proceed through each tab in turn.

### Application Servers

This tab is used to configure the Web Servers, on which the Application Server component is installed.

1. In the left of the window is a list of servers in the cluster, check the server which is to be the Side A Web Server.
2. Use the arrow button to move it to the **Primary Application Servers** list.
3. If there is a Side B Web Application Server, check the **Dual-sided** check box. Select the server which is to be the Side B Web Server and move it to the **Secondary Application Servers** list.

### UCCMP Database

This tab is used to configure the Unified CCMP databases.

1. Click the **UCCMP Databases** tab. A table displays with four columns that contain information about the databases after they have been configured.
2. To add a new database server, click **New**. The **UCCMP Database Configuration** window displays.

   **Note:** The first database to be configured must be the publisher. For replicated systems, enter the subscriber details after the publisher has been created.

3. Enter the following details:
   - **Server** Select the server that the database is installed on from the drop-down list of the servers you configured on the **Servers** tab earlier. This defaults to the current machine.
   - **Catalog** Enter the name of the database in the field provided. This defaults to **Portal**.
   - **Default Database Connection Parameters** Select the radio button of the login credentials you want to be used as a default by Unified CCMP cluster components when no other credentials are available.
     - **Windows authentication** select this option to use windows authentication
     - **SQL Server authentication** This is the recommended option for most installations. Enter the **Login Name** and **Password** in the fields provided.

       **Note:** The OLAP details are not required for this version of Unified CCMP.
4. Click **OK.**

For a dual-sided system, after the publisher database has been set up, you can configure replication. Replication must be configured before Unified CMs and either NAMs or Unified ICMs are added to the cluster.

### UCCMP Database Replication

To configure replication, *remain in the UCCMP Database* tab and perform the following steps.

Before configuring replication, check that the SQL Server Agent service is running:

1. Click **Start > Run**
2. Enter **Services.msc** and then click **OK.**

3. Confirm the **SQL Server Agent** service is in the **Started** state. If SQL Server Agent is not started, right click the service name and click **Start.**

To configure Unified CCMP database replication:

1. Click **Replication.** The UCCMP Database Replication Configuration window opens and displays all the selected server details. Perform any modifications at this stage if necessary.

   **Note:** If you have chosen to set up Reporting Services Replication before UCCMP Database Replication, then values here will be inherited from the Reporting Services Replication setup. This will not affect the normal running of the system.

2. Click **Replicate** (if asked to save changes, click **Yes**) and confirm. This will open a work execution window that will show the progress statuses for replication.
3. To start the replication configuration process click **Execute**. When asked to confirm replication, click **Yes**. After replication is set up successfully click **Close**.
4. Click **OK** to close the Unified CCMP Database Replication Configuration window.
5. Click **Close** to close the UCCMP Configuration Window.
6. Log in to the Side B database server (the subscriber) and open the **SQL Server Management Studio**.
7. Right-click the Replication folder and then click **Launch Replication Monitor**. The Replication Monitor displays.
8. Expand **My Publishers**. If the Side A database server publisher is not shown then it must be added:
   a. Right-click **My Publishers > Add Publishers**. The Add Publisher dialog displays.
   b. Click **Add > Add SQL Server Publisher**.
      - **Server Name** Enter the name of the Side A (publisher) server.
      - **Authentication** Enter authentication details to connect to the server.
9. Click **Connect**. If a notification message about the distributor location is displayed, click **OK** and provide connection details for the distributor.
10. Click **OK** to add the publisher to the list of monitored publishers.
11. Navigate to the snapshots listed below the Publisher. Two snapshots display called:
    - [Portal] Base
    - [Portal] Non Queued

12. Click on the base publication snapshot then click on the **Warnings and Agents** tab.
13. Right-click on the Snapshot Agent in the Agents and Jobs list and click **Start Agent.** Wait for the status to change to 'Completed'. This may take several minutes.
14. Repeat steps 12 and 13 for the Non Queued snapshot.
15. Exit the Replication Monitor and close SQL Server Management Studio.

Unified CCMP database replication setup is now complete.

### Reporting Services Servers

Use this tab to configure the location of the SQL Server Reporting Services report server.

1. Click **New**.
2. Select the server from the drop-down list.
3. Click **Test** to check the connection.
4. Click **OK**.
5. Repeat until all servers hosting Reporting Services have been entered.

**Note:** Connections to the Reporting Services Web Service may only be performed over an HTTP connection. Connections via HTTPS are not supported. Ensure that the Report Server URL is configured to use an HTTP connection.

### Report Server Databases

This tab is used to enter details of the configured Reporting Services database servers. These will usually be the same servers as the Unified CCMP database servers.

Add each Report Server database server to the list. The first server you add will automatically be selected as the Replication Publisher.

6. Click the **Report Server Databases** tab.
7. Click **New**. The Report Server Database Configuration dialog box displays.
   a. **Server** Choose the Side A database server
   b. **Authentication** Choose windows authentication.
8. Click **OK**.

For a dual-sided system, repeat the process adding the Side B report server database.

### Report Server Database Replication

If you are configuring a dual-sided Unified CCMP system, you must use the Configuration Manager tool to replicate the Report Server databases.

In the Report Server Databases tab, click **Replication**. The Report Server Database Replication Configuration window displays.

1. Click **Replicate**; if asked to save pending changes, click **Yes**.
2. To start the replication configuration process click **Execute**.

3. You will be asked to take a backup of the report server encryption key from the Publisher before setting up replication.
4. To *back up* the report server encryption key do the following:
   a. Log in to the Side A web server; this is the *publisher* side.
   b. Click **All Programs > Microsoft SQL Server 2005 > Configuration Tools > Reporting Services Configuration**. The Reporting Services Configuration Manager displays.
   c. In the Instance Selection window, select the Publisher and click **Connect**.
   d. Click **Encryption Keys**; the Encryption Key window displays to the right.
   e. Click **Backup**.
   f. Enter a password.
   g. Click **…** (to the right of Key File).
   h. Enter a File name; make a note of it for future reference (this will have the **.snk** extension file name).
   i. Click **OK**.
   j. **Exit** the Reporting Services Configuration tool.
5. Return to the Report Server Database Replication Manager.
6. Confirm that you have backed up the report server encryption key. If replication is successful, you will see a message in the Report Server Database Replication Manager window saying you should restore the encryption key from the publisher report server to all configured subscribers.
7. To *restore* the report server encryption key do the following:
   a. Log in to the Side B web server; this is the *subscriber* side.
   b. Click **All Programs > Microsoft SQL Server 2005 > Configuration Tools > Reporting Services Configuration**. The Reporting Services Configuration Manager displays.
   c. In Instance Selection window, select the Subscriber and click **Connect**.
   d. Click **Encryption Keys**, the Encryption Key window displays to the right.
   e. Click **Restore**.
   f. Enter the password.
   g. Click **…** (to the right of Key File).
   h. Locate the **.snk** file containing the encryption key.
   i. Click **Open**.
   j. Click **OK**. The restoration of the encryption key is complete.
   k. **Exit** the Reporting Services Configuration tool.
8. Return to the Report Server Databases tab.

### UCCMP Provisioning

Use this tab to configure the location of the Provisioning Server.

1. Click **New**.

2. Enter the following details:
    - **Server** Select the server on which the Unified CCMP Provisioning Server component has been installed from the drop-down list.
    - Ensure the **Enabled** check box is checked.
3. Click **OK.**

If there is a Side B Provisioning Server, repeat these steps for the Side B Provisioning Server.

## Communications Servers

This section will configure the connection to the Unified CCE servers in the network (for example, routers). Primarily Unified CCMP will connect to a standard Unified CCE; however it also supports a number of different configurations:

- Unified CCE: This configuration is used for smaller enterprise level deployments (normally those with less than 8000 agents) and has one ICM instance.
- Unified CCE Parent/Child: This configuration is used for larger deployments (those that exceed 8000 agents or require geographical separation). The parent Unified ICM serves as the network or enterprise routing point and can route between many children. The child Unified ICM can receive calls direct as well as calls routed from the parent; it is unaware of any other children (the child is best viewed as a standalone Unified ICM).
- Hosted deployments of Unified CCE: This configuration is largely the same as the Unified CCE, but it supports multi-tenant or shared servers to manage multiple customer instances. It will also require the creation of a NAM; this is covered in NAMs section below. **Note:** A NAM must be added before any associated CICMs.

### Unified ICM

This tab is used to configure the Unified ICM instances configured in the Unified CCE deployment.

1. Click the **Unified ICM** tab. A table displays, with seven columns that will show information about the Unified ICMs after they have been configured.
2. To create a new CICM instance, click **New**. The **CICM Database Configuration** window displays.
    - **Instance Name** Enter a unique name to represent the Unified ICM in Unified CCMP.
    - **Server** Select the server that is hosting the Unified ICM from the drop-down list of the servers you configured on the **Servers** tab earlier.
    - **Database Connection Parameters** Select the radio button of the login credentials you want to apply:
        - **Windows authentication**
        - **SQL Server authentication** This option must only be selected 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.

- **ICM Instance** Select the correct Unified ICM to use from a drop-down list of those available on the selected server.
- **HDS** This setting is not used.
- **AWDB Catalog** The name of the Administration & Data Server database catalog, such as `<instance>_`awdb. This is configured automatically.
- **HDS Catalog** The name of the historical data server catalog, such as `<instance>_`hds. This is configured automatically.
- **Common ConAPI Credentials** Set up the credentials required to connect to the Unified ICM. These fields are dimmed until the Provisionable check box has been checked.
    - **Application Name** Enter the name of the application you created on the Unified ICM earlier.
    - **Application Key** Enter the password of the application you created on the Unified ICM earlier.
    - **Remote Registry Port** The port to connect to on the Unified ICM. This value will default to 2099, but must be updated to the Administration & Data Server RMI Registry port configured using the Unified ICM CMSControl tool earlier on. This port must be unique to the specific Administration & Data Server including dual-sided Unified ICM configurations. **Note:** The Windows Server 2008 firewall will not allow traffic through this port by default. If Windows firewall is switched on a firewall rule must be created to allow inbound TCP traffic on the port used here.
    - **Local Registry Port** Use the same as the Application RMI registry port set up in the CMS Control Console earlier. Usually the same port number as the Remote Registry Port entered above.
    - **Local Port** This port number will be used by the Unified ICM Administration & Data Server to communicate with the Unified CCMP Provisioning Server. By default this port will be set to 3333 for the Unified CCMP A side and 3334 for the Unified CCMP B side. The local port property must be unique for each Administration & Data Server. For example, a dual-sided installation with two Unified ICMs configured, will have a different local port specified for each Administration & Data Server it is connected to; there will be a total number of four different ports. **Note:** The Windows Server 2008 firewall will not allow traffic through this port by default. If Windows firewall is switched on a firewall rule must be created to allow inbound TCP traffic on the port used here.
- **Provisionable** This indicates that the Unified ICM is to be provisioned by the Portal, and must be checked.
- **NAM Based** Check this box if the CICM is NAM based.

- **Dual-sided** Check this box if you are using a dual-sided Unified ICM. You will then be able to fill in details for Side B.
- **Self-Skilling Enabled** Check this box to enable the Agent Self Re-Skilling feature of Unified CCMP. Enabling this option will limit Unified ICM provisioning requests to one every 30 seconds.
- **Multi Media Support** Check this box if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance in order to provide support for non-voice interactions.

3. Click the **Configure Active Directory Mapping** button. The **Browse Active Directory** window displays. This is used to associate the domain users who are required for supervisor memberships to supervisor agents. The domain user must be a member of the domain active directory.
   - **Domain Controller A** Enter the name of the Domain Controller.
   - **Domain Controller B** Enter the name of the Side B Domain Controller if present.
   - **Use Secure Authentication** Check this check box in order to log in to the domain controller as a specified user.
   - **Username** Enter the name of the domain user, such as CICMSERV\administrator.
   - **Password** Enter the domain user's password.
4. Click **Refresh**.
5. Navigate to the Active Directory folder corresponding to the Unified ICM instance.
6. Click **OK**, and **OK** again to save the new Unified ICM.

### NAMs

**Note:** This tab is only relevant to hosted Unified CCE.

To configure a NAM do the following:

1. Click the **NAM** tab. A table displays with seven columns that will show information about the NAMs after they have been configured.
2. To create a new NAM instance, click **New**. The **NAM Configuration** window displays.
   - **Instance Name** Enter a unique name to represent the NAM instance.
   - **Server** Select the server that is hosting the NAM from the drop-down list of the servers you configured on the **Servers** tab earlier.
   - **Database Connection Parameters** Select the radio button of the login credentials you want to apply:
     - **Windows authentication**.
     - **SQL Server authentication** This option must only be selected 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.

- **Unified ICM Instance** Select the correct Unified ICM to use from a drop-down list of those available on the selected server.
- **HDS** In some deployments, real time and historical data may be held separately. Check this box if the specified NAM holds *only* historical data.
- **AWDB Catalog** The name of the Administration & Data Server database catalog, such as nam_awdb. This is configured automatically.
- **HDS Catalog** The name of the historical data server catalog, such as nam_hds. This is configured automatically.
- **Common ConAPI Credentials** Set up the credentials required to connect to the NAM.
  - **Application Name** Enter the name of the application you created on the NAM earlier.
  - **Application Key** Enter the password of the application you created on the NAM earlier.
  - **Remote Registry Port** The port to connect to on the NAM. Use 2099.
  - **Local Registry Port** Use the same as that set up in the CMS Control Console earlier. The port must be unique for each NAM.
- **Provisionable** This indicates that the NAM is to be provisioned by the Unified CCMP, and must be checked.
- **Dual-sided** Check this box if you are using a dual-sided NAM. You will then be able to fill in details for Side B.
- **Multi Media Support** Check this box if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance in order to provide support for non-voice interactions.

3. Click the **Configure Active Directory Mapping** button to open the **Browse Active Directory** window. This is used to provision the domain users who are required for supervisor memberships. The domain user must be a member of the domain active directory.
   - **Domain Controller A** Enter the name of the Domain Controller.
   - **Domain Controller B** Enter the name of the Side B Domain Controller if present.
   - **Use Secure Authentication** Check this check box in order to log in to the domain controller as a specified user.
   - **Username** Enter the name of the domain user, such as NAMSERV\administrator.
   - **Password** Enter the domain user's password.
4. Click **Refresh**.
5. Navigate to the Active Directory folder corresponding to the NAM instance.

6. Click **OK** twice to save the new NAM.

### Unified CMs

To configure a Unified CM do the following:

1. Click the **Unified CMs** tab. A table displays with two columns, which show information about the Unified CMs after they have been configured.
2. To add a Unified CM click **New.**
3. When prompted to import the Tenant/Peripheral data click **Yes.**

**Note:** The Tenant/Peripheral data import is a necessary step during the initial configuration.

**Note:** If the import is not complete within a few minutes, this may be because the Data Import Service has not been stopped. Stop the service from the **services.msc** command line and attempt the data import again.

4. In the Unified CM window:
   - **Instance Name** Enter the name to be used for the Unified CM instance by the Configuration Management utility.

     **Note:** For simplicity of future maintenance, this name must be the same as the appropriate Unified ICM instance name.
   - **Server** Select the server hosting the Unified CM that you configured on the Servers tab earlier.
   - **Version** Select the required Unified CM version option. The following table describes which Unified CM versions map to each version option displayed in the Configuration Manager.

| Unified CM Version | Version |
|---|---|
| All Unified CM 5.x versions | 5.x |
| All Unified CM 6.0.x versions | 6.0.x |
| All Unified CM 6.1.x versions | 6.1.x |
| All Unified CM 7.x versions | 7.x |
| All Unified CM 8.0.x versions | 8.0.x |
| All Unified CM 8.5.x versions | 8.5.x |
| All Unified CM 8.6.x versions | 8.5.x |

   - **Endpoint** Enter the URL used to access the Unified CM AXL interface. The default is the default URL for the Unified CM version selected.
   - **User Name** Enter the name of the Unified CM Administration user. This is the user name that the Unified CCMP Data Import Server will use when connecting to the Unified CM web service.
   - **Password** Enter the Unified CM Administrator user's password.

- **Test** Click to test the connection to the configured Unified CM.
- **Provisionable** This indicates that the **Unified CM** is to be provisioned by the Portal, and must be checked.

5. Select the associated Unified ICM and tenants from the drop-down list, and click **Add**. This will associate the Unified CM with the tenant to which it belongs.
6. Select the associated peripherals and their PG Users from the drop-down list and click **Add.**
   - **PG User** Enter the name of a directory user on the Unified CM with whom new phones will be associated when they are created through the Unified CCMP user interface. In order for the Unified ICM to control the new phone, it must be added to a specific user's list of controlled devices in the directory on the Unified CM. You can find a list of directory users by logging in to Unified CM Administration (normally https://<*SERVER*>/ccmadmin, for example https://CCMSERV ccmadmin).
7. Click **OK.**
8. When you have finished adding Unified CMs, ensure the **Management Portal Data Import** service has restarted.

## Connection Manager

Click **Connection Manager** to monitor the status of connections.

The connections between servers are normally created automatically, but if necessary you can manually create individual connections by clicking **New**, entering the **Connection Source** and **Connection Target**, and clicking **Create All Connections.**

**Note:** In some cases, such as where the source and/or target are dual-sided, more than one connection may be created.

The connection types are:

- IN Datasource
- Unified ICM /NAM AWDB
- Unified ICM /NAM HDS
- Unified CM

The **Connections by Server** tab is not relevant to this version of Unified CCMP.

## Global Properties

This configures advanced properties. For most installations there is no need to edit these properties.

- **Java RMI Server Host Name** This may need to be configured in cases where the Database Server has two network cards. Enter the IP address to be used by the ConAPI connection from the Unified ICM.
- **Additional VM Parameters** Indicates any additional parameters for use when connecting to the Java Virtual Machine.

**Caution** The default parameters of -Xrs must not be deleted. Deleting these parameters might result in problems with the Data Import service.

## Saving the Configuration

Click **Save** to save your configuration. Unified CCMP is now configured to manage the Unified CCE and Unified CM instances that you have specified using the Configuration Manager tool.

Please see Chapter 6, Post-Installation Steps, for information on preparing Unified CCMP for first use.

# 6. Post-Installation Steps

## Starting the Unified CCMP Services

Before proceeding to log in to Unified CCMP, check that the Unified CCMP Windows services are running on the Unified CCMP Servers.

To check that a service is running:

1. Click **Start > Run**
2. Enter **Services.msc** and then click **OK.**
3. Confirm the service is in the **Started** state. If a service is not started, right-click the service name and click **Start.**

The following services should be running on the **web servers**:

- UCCMP: System Monitoring Services
- UCCMP: Scheduling Services
- UCCMP: Reporting Services
- UCCMP: Application Search Services

The following services should be running on the **database servers**:

- UCCMP: Data Import Server
- UCCMP: Partition Table Manager
- UCCMP: Provisioning Server

When all services are running Unified CCMP is ready for use.

**Note:** If you have just started the System Monitoring Service and Application Service on the web server, you will need to wait a few minutes before logging in to allow the services to load completely.

## Logging in to Unified CCMP

Unified CCMP can now be opened from **Start > All Programs > Management Portal > Web > Management Portal**. This opens a web page that you can bookmark.

**Note:** As Unified CCMP must perform a number of system operations after configuration, it may take some time before you can access your imported Unified CCE data when you first log in.

To log in to a new system, use the username ‘administrator’ and a blank password. You will be prompted to change this. If you are logging in to an upgraded system, the administrator password will not have changed from that previously used.

**Note:** If you lose the administrator password, it can be reset by another user with equal permissions; note down the chosen password and keep it somewhere secure.

Information on how to set up tenants and other necessary items within the Management Portal can be found in the *Administration Manual for Cisco Unified Contact Center Management Portal*.

## Report Uploading

To enable audit reporting, the audit report templates must be uploaded into the system. To upload the reports into the Unified CCMP system, perform the following steps on the web server. In a dual-sided system these steps need to be performed on the Side A web server only.

1. Click **Start** > **All Programs** > **Management Portal** > **Report Uploader** > **Audit Report Uploader.** The **Upload Audit Reports** window displays.
2. Enter **administrator** in the **User Name** field.
3. Enter your administrator password in the **Password** field.

**Note:** You must have specified a new administrator password in the Management Portal, as described above, in order to perform this task.

4. Click **Upload.**

The Report Uploader transfers the report template from the folder in which it was installed to a shared folder for users to access.

## Unified CVP Media File Upload

The Unified CCMP media file upload feature provides the capability to provision WAV announcement files directly to a Unified CVP Server. This allows the associated WAV announcement for a Network VRU Script in the Unified ICM to be replaced in near real-time.

This section describes how to configure a Windows Distributed File System for Unified CCMP to write media files to, and for Unified CVP to read media files from.

This solution requires your Unified CVP Servers to be hosted on Microsoft Windows Server 2003. Both the web servers hosting Unified CCMP and the Unified CVP Servers must belong to the same domain. This domain may be a Windows 2003 or Windows 2000 domain controller.

Announcements are written to a domain share called **PortalMedia** that must exist on the domain controller. Use the Microsoft Distributed File System to provide access to the file system on the Unified CVP Servers. If multiple Unified CVP Servers are being used then Microsoft File Replication can be used to ensure that announcement files are maintained in all the correct places.

Below is a brief description of how to set up the Microsoft Distributed File System and Microsoft File Replication for this application.

### Preparing the Configuration

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

- Make a note of the **Host Name** and **IP Addresses** of ALL of the machines that are hosting Unified CVP.
- Make a note of the **User Name** and **Password** of an administrative user on the domain so that you can configure *File Replication* and the *Distributed File System.*

- Ensure that the **Distributed File System**, **File Replication** and **Remote Procedure Call** services are running on all of the Unified CVP Servers and the Domain Controller.

## Configuring Distributed File System for Unified CVP Media File Upload

This will take you through the process of adding a shared folder for each Unified CVP Server in the domain. It will then create a domain level share for these file destinations.

1. Log in 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 the **Distributed File System** node in the left of the screen and select the **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.

## Configuring DFS Root Targets

For each media server that the Unified CVP Media File Upload should add files to, perform the following actions:

1. Right-click the new root and select the **New Root Target** option from the menu.
2. Enter the **Server Name** for the Unified CVP 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.

Once complete, a Distributed File System (DFS) path is available for Unified CCMP to upload files to. This will be in the \\<DomainName>\PortalMedia form and will have full access for all machines in the domain.

### Configuring File Replication for Unified CVP Media File Upload

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

The following steps take you through the process of replicating files between the DFS shares. To enable this functionality, you need to ensure that the File Replication service is set to **Automatic** and is currently running. To begin file replication perform the following steps:

1. Log in 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 the **Distributed File System** node in the left panel and select the **Show Root** option.
4. Select the **PortalMedia** node.
5. Right-click the **PortalMedia** node located in the left of the **Distributed File System** window. Select the **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 the **Full Mesh** topology for the replication set.
8. Click the **Finish** button to set up replication between the selected folders.

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

## Support for Additional Languages

The Unified CCMP web user interface provides support for the following languages:

- Danish
- Dutch
- French
- French Canadian
- German
- Italian
- Japanese
- Korean
- Portuguese
- Russian
- Spanish
- Swedish
- Simplified Chinese
- Traditional Chinese

To support these languages the Unified CCMP Language pack installer must be executed on all of the Web/Application Servers within the installation. This installer is located on the Unified CCMP DVD in the Languages folder.

**Note:** English customers do not need to run the Language Pack installer as English is the default language installed with Unified CCMP.

For upgrades of existing Unified CCMP installations, user must uninstall existing versions of the Unified CCMP Language Pack before performing an upgrade. After the upgrade is complete, the latest version of the Language Pack must be installed to support the required languages.

User language specifications may be set after a user has logged in, by navigating to the **Settings > User Settings** page and selecting the appropriate culture from the drop-down list before clicking **Save**.

## Validating the Unified CCMP Installation

Following an installation or upgrade, check that the system is functional by executing the following tests:

| Check | Success Criteria |
|---|---|
| **Unified CCE Provisioning** | |
| Log in to the Side A web server and create a new Skill Group. This tests provisioning from the A Side web server. Run this test against each configured UCCE instance. | The skill group should be successfully created. |
| [Dual-sided system only]<br>Log in to the Side B Web Server. Locate the Skill Group created in the previous test. This tests replication of the change from the A side to the B side. | The skill group should be visible on the B Side. |
| [Dual-sided system only]<br>Log in to the Side B web server and create a new Skill Group. This tests UCCE provisioning from the B Side web server. | The skill group should be successfully created. |
| [Dual-sided system only]<br>Log in to the Side A Web Server. Locate the Skill Group created in the previous test. This tests replication of the change from the B side to the A side. | The skill group should be visible on the A Side. |
| Create a new Skill Group on the AW using the Cisco Skill Group Explorer tool. Wait 30 minutes and check that the Skill Group is imported into Unified CCMP. | The skill group should be visible on the A and B Side (if present). |
| **Unified CM Provisioning** | |
| Log in to the Side A web server and create a new IP Phone. This tests Unified CM provisioning from the A Side web server. | The IP Phone should be successfully created. |

| | |
|---|---|
| [Dual-sided system only]<br>Log in to the Side B web server and create a new IP Phone. This tests Unified CM provisioning from the B Side web server. | The IP Phone should be visible on the B Side. |
| **Reporting** | |
| Log in to the Side A Web Server and run an audit report. This tests that reports can be run successfully from the Side A Web Server. | The report should run and return data if there is data available for the period. |
| [Dual-sided system only]<br>Log in to the Side B Web Server and run an audit report. This tests that reports can be run successfully from the Side B Web Server. | The report should run and return data if there is data available for the period. |
| [Dual-sided system only]<br>Log in to the Side A Web Server and create a saved link to an audit report. This tests that reports are replicated from the A Side to the B Side. | The link should be visible on the Side B web server after a short interval. You may need to refresh your browser before the link is visible. |
| [Dual-sided system only]<br>Log in to the Side B Web Server and create a saved link to an audit report. This tests that reports are replicated from the B Side to the A Side. | The link should be visible on the Side A web server after a short interval. You may need to refresh your browser before the link is visible. |

## Security Hardening

Unified CCMP servers may be configured in line with the following NSA (National Security Agency) guides for customers with additional security hardening requirements.

.NET 2.0 Hardening Guide
http://www.nsa.gov/ia/_files/app/I731-008R-2006.pdf

SQL 2005 Hardening Guide
http://www.nsa.gov/ia/_files/db/I733-042R-2008.pdf

# 7. Upgrading from a Previous Version

This chapter details how to upgrade from previous Unified CCMP versions to Release 8.5(2).

## Overview

Unified CCMP versions prior to 8.5(2) ran on the 32-bit version of Windows Server 2003. Unified CCMP 8.5(2) runs on Windows Server 2008 R2 for which Microsoft do not support cross-architecture in-place upgrades. This means that an operating system reinstall is required to upgrade to Unified CCMP 8.5(2).

To upgrade Unified CCMP, a backup of the Unified CCMP and Microsoft Reporting Services databases must be taken prior to commencing the upgrade. After the operating system, SQL Server prerequisites and the Unified CCMP 8.5(2) Database component are installed the database backups can be restored and upgraded as part of the installation process.

**Caution:** Ensure that you have up-to-date backups of all Unified CCMP databases before you begin.

### Upgrade Checklist

This checklist describes the steps that will be performed during the upgrade and can be used to track progress through the upgrade and ensure that no steps are missed. Depending on the version you are upgrading from, and the deployment model you have, some steps will not apply.

| Step | Complete |
|---|---|
| **Before Upgrading** | |
| Stop the Unified CCMP Services | |
| [Dual-sided Systems Only] Unreplicate databases | |
| Backup the Portal and Reporting Services Databases | |
| Install and configure Windows 2008 Server R2 on the Unified CCMP servers. | |
| Install SQL Server 2005 | |
| Restore the Reporting Services Databases | |
| Configure Reporting Services ([SQL Server 2000 Systems Only] upgrade the Reporting Services databases). | |
| [SQL Server 2000 Systems Only] Update the ReportServerTempDB (Microsoft KB# 946741). | |
| Configure access for the Network Service account to the Reporting Services database. | |
| **Installing Unified CCMP** | |
| Install the Unified CCMP 8.5(2) prerequisite software. | |
| Install the Database Install Tool on the Side A database server. | |

| Step | Complete |
|---|---|
| Install the Unified CCMP 8.5(2) database on the Side A database server. | |
| [Dual-sided Systems Only] Install the Database Install Tool on the Side B database server. | |
| [Dual-sided Systems Only] Install the Unified CCMP 8.5(2) database on the Side B database server. | |
| [Dual Tier Systems Only] Grant the Reporting Services execution account permissions on the Portal databases. | |
| [Dual Tier Systems Only] Grant the Database Server Network Service account permissions on the ReportServer databases. | |
| Restore the Portal database backup on the Side A database server. | |
| Upgrade the Portal Database on the Side A database server. | |
| [Dual-sided Systems Only] Install the Database Install Tool on the Side B database server. | |
| [Dual-sided Systems Only] Install the Unified CCMP 8.5(2) database on the Side B database server. | |
| [Dual-sided Systems Only] Restore the Portal database backup on the Side B database server. | |
| [Dual-sided Systems Only] Upgrade the Portal database on Side B. | |
| Install the Application Server component. | |
| Install the Web Server component. | |
| Install the Data Import Server component. | |
| Install the Provisioning Server component. | |
| [Dual-sided Systems Only] Install the Unified CCMP components on Side B. | |
| Configure Unified CCMP 8.5(2) | |
| [Dual-sided Systems Only] Re instantiate Portal database replication using the Unified CCMP Configuration Management tool. | |
| Add the Report Server databases to the CCMP cluster using the Unified CCMP Configuration Management tool. | |
| [Dual-sided Systems Only] Replicate the Reporting Services Databases. | |
| **Confirm the Successful Upgrade** | |
| Check all required services are running. | |
| Test that the upgrade has succeeded. | |

# Upgrade Procedure

This section describes the procedure for upgrading Unified CCMP.

Before you start, ensure that you have the cryptographical password you entered when you first installed the Unified CCMP database component because this will be required during the upgrade.

This procedure covers both single-sided and dual-sided deployment models. The term 'Side A' applies to both the A Side of a dual-sided installation and a single sided installation.

## Before Upgrading

Unified CCMP 8.5(2) runs on the Windows Server 2008 R2 (64-Bit) operating system. Before the Unified CCMP 8.5(2) components can be installed, the Unified CCMP and Reporting Services databases must be backed up and copied to a safe location so that the Windows operating system upgrade can be carried out. Prior to backing up the databases, the Unified CCMP services must be stopped and if the system is dual-sided, the databases must be unreplicated.

### Stopping the Unified CCMP Services

Before starting the upgrade the Unified CCMP services must be stopped on all servers.

To stop the Unified CCMP: Data Import Server service, proceed as follows:

1. On the Side A database server, click **Start** > **Run**. The **Run** window displays.
2. In the **Open** field, enter **services.msc**. The **Services** window displays.
3. Right-click the **UCCMP: Data Import Server** service from the list of services. **Note:** In older versions of Unified CCMP this service appears as **Management Portal: Data Import Server**.
4. Click **Stop.**

Repeat this process for all running Unified CCMP services on the database server.

Close the **Services** window.

For dual-sided installations, repeat this process on the Side B database server.

To stop the Unified CCMP: Monitoring Service, the Unified CCMP: Application Search Server service, and the Unified CCMP: Reporting Services service, proceed as follows:

1. On the Side A web server, click **Start** > **Run**. The **Run** window displays.
2. In the **Open** field, enter **services.msc**. The **Services** window displays.
3. Right-click and click **Stop** on each of the **Unified CCMP** services from the list. **Note:** In older versions of Unified CCMP these services appear as **Management Portal: <SERVICE NAME>**

Close the **Services** window.

For dual-sided installations, repeat this process on the Side B web server.

### Removing Portal Database Replication

**If you have a dual-sided installation then you must follow these steps to remove replication.**

Follow these steps to remove replication from the Portal databases.

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 > All Programs > Management Portal > Configuration Manager**. **Note:** In some earlier versions of Unified CCMP this tool is called **Cluster Configuration**.
3. Click **UCCMP Servers**. **Note:** In some earlier versions of Unified CCMP this step is not required.
4. Select the **UCCMP Database** tab. **Note:** In some earlier versions of Unified CCMP this tab is labeled **Portal Database**.
5. Click **Replication**.
6. Click **Unreplicate**.
7. Click **Yes** when prompted to remove replication. **Note**: Removing replication may take some time.
8. After replication has been successfully removed, click **OK** to close the Replication dialog box.

### Removing Reporting Services Replication

**If you have a dual-sided installation of Unified CCMP version 8.0 or above Reporting Services replication must also be removed.**

Once replication has been successfully removed then you may close the Configuration Manager.

Follow these steps to remove replication from the Reporting Services databases.

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 > All Programs > Management Portal > Configuration Manager**.
3. Click **UCCMP Servers**.
4. Select the **Report Server Databases** tab.
5. Click **Replication**.
6. Click **Unreplicate**.
7. Click **Yes** when prompted to remove replication

**Note** Removing replication may take some time.

After replication has been successfully removed then you may close the Configuration Manager.

### Backing up the Databases

Back up the Portal and Report Server databases and copy the backups to a safe location where they can be accessed once the Windows 2008 Server Operating System has been installed.

1. On the Side A database server click **Start > All Programs > Microsoft SQL Server > Enterprise Manager** (for installations using SQL Server 2005 then you must select **Start > All Programs > Microsoft SQL Server 2005 > SQL Server Management Studio**).
2. Navigate to **Portal** database.

   Right-click **Portal** and select **Tasks > Backup.** Save the **.bak** file to a suitable location.

Repeat this process for the ReportServer and ReportServerTempDB databases.

For a dual-sided system repeat the back up process for the Side B database server.

### Windows Server 2008 R2 Installation

After the database backups have been taken and stored in safe location, install Windows Server 2008 R2 on the Unified CCMP Servers.

Apply the Windows post-installation configuration steps for Unified CCMP described in the Server Requirements section of Chapter 2.

### Installing Microsoft SQL Server 2005

Install Microsoft SQL Server 2005 and Microsoft SQL Server 2005 SP4 as described in Chapter 3 Microsoft SQL Server Setup but **do not** execute the steps in the SQL Server 2005 Reporting Services Configuration/Reporting Services Configuration Section. Instead follow the steps described in the Reporting Services Configuration section below to configure Reporting Services after restoring the Reporting Services databases.

### Restoring the Reporting Services Databases

After the operating system and SQL Server components are in place it is necessary to restore the database backups taken prior to the operating system installation.

Perform the following steps to restore the backups of the ReportServer and ReportServerTempDB databases.

To restore a database:

1. On the Side A database server, click **Start > All Programs > Microsoft SQL Server> Management Studio**.
2. Right click **Databases** and select **Restore Database**.
3. In the Restore Database window choose **From Device** and **Add** the location of the backup file from the same side database server.
4. Select the backup file to restore the database from and click **OK**.
5. Check the check box next to the backup set you just added and click **OK**.
6. Select the database to restore to from the **To Database** drop-down list.
7. Click **OK** to start the restore.

For dual-sided systems, repeat these steps, restoring the Side B Reporting Services database backups to the Side B database server.

### Reporting Services Configuration

Configure Reporting Services as follows.

1. On the Side A Web Server select **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > Reporting Services Configuration**. The Reporting Services Configuration Manager displays.
2. Click **Connect** to select the local Report Server instance. The Reporting Services Configuration Manager loads the instance configuration information.
3. Configure the Report Server Virtual Directory:
    a. In the left panel select **Report Server Virtual Directory**. The Report Server Virtual Directory Settings window displays.
    b. Click **New**. The Create a New Virtual Directory window displays with the default Virtual Directory name of ReportServer. Click **OK**. The ReportServer virtual directory is created.
4. Configure the Report Manager Virtual Directory:
    a. In the left panel select **Report Manager Virtual Directory**. The Report Manager Virtual Directory Settings window displays.
    b. Click **New.** The Create a New Virtual Directory window displays with the default Virtual Directory name of Reports. Click **OK.** The Reports virtual directory is created.
5. Configure the Web Service Identity:
    a. In the left panel select **Web Service Identity**. The Web Service Identity window displays.
    b. Click **New** next to Report Server to create a new application pool for the Report Server.
    c. Enter a name, such as ReportServer, for the application pool.
    d. Select **Built In Account**.
    e. Select **Local System.**
    f. Click **OK.**
    g. Click **New** next to Report Manager to create a new application pool for the Report Manager.
    h. Enter a name, such as ReportManager, for the application pool.
    i. Select **Built In Account**.
    j. Select **Local System.**
    k. Click **OK.**

l. Click **Apply** to configure the identity for the new virtual directories. When the configuration is complete a green tick displays to confirm that the identity has been set correctly.

6. Set up the ReportServer database:
    a. In the left panel select **Database Setup**. The Database Connection window displays.
    b. Enter the name of the Side A database server in **Server Name**.
    c. Click **Connect** and confirm the credentials that will be used to access the database. These credentials will be used to connect to the database server and update the ReportServer database.
    d. Ensure the **Database Name** is **ReportServer**.
    e. Some older versions of Unified CCMP ran on SQL Server 2000. If the Unified CCMP system that you are upgrading from was an SQL Server 2000 system click **Upgrade** and **OK** when prompted to confirm the upgrade. **Note:** If the upgrade fails, see the Reporting Services Database Upgrade Fails section in Chapter 9, Troubleshooting. The upgrade has failed if a warning message is shown in the Task Status window next to the 'Upgrading the Reporting Services database' task. The upgrade has succeeded if a green tick mark icon is displayed next to the 'Upgrading the Reporting Services database' task.
    f. Click **Apply** to associate the database to the Report Server.
7. It is also necessary to delete the old encryption keys and set up new ones. From the **Reporting Services Configuration Manager** select **Encryption Keys**.
    a. Click **Delete**.
    b. Click **OK** to confirm deletion of encrypted content.
8. Configure the Reporting Services Execution Account:
    a. Click the **Execution Account** option from the list on the left of the window. Check the check box for **Specify an execution account** and enter the domain account information for the execution account. The Reporting Services Execution Account is used is used by Microsoft SQL Server Reporting Services to authenticate requests when establishing the database connection used for audit reporting in Unified CCMP. See Required Domain User Accounts in Chapter 2 for further details on creating the Reporting Services Execution Account user account.
    b. Click **Apply**.
9. Click **Exit** to close the Reporting Services Configuration Manager.

For dual-sided systems repeat the process on the Side B web server.

### Updating the ReportServerTempDB schema

If you are upgrading Unified CCMP from a version that ran on SQL Server 2000 there is a known Microsoft issue that affects the Reporting Services ReportServerTempDB. The issue is caused by a difference in the schema between

the two versions. The ReportServerTempDB database schema must be updated to correct this issue.

Steps for resolving this can be found at: http://support.microsoft.com/kb/946741.

**Note:** These steps must be applied **after upgrading and before replicating** the ReportServer database.

## Installing Unified CCMP

### Prerequisites

Review the list of prerequisite software described in Chapter 2 and install the remaining prerequisites on the Unified CCMP servers.

### Database Component

To install the Unified CCMP Database component, perform the following steps.

1. On the Side A database server insert the Unified CCMP installation media. The installer should launch automatically. If it does not, browse the installation CD in Windows Explorer and double-click **autorun.hta**.
2. Select the **Database Component** tab, click **Run Test** to check for prerequisites, and click **Install**. Click **Next** to go through each window in turn.
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. Read it thoroughly before accepting.
4. In the **Cryptography Configuration** window:

   **Passphrase** Enter the cryptographical passphrase you created during installation of the Database Server component **when you first installed CCMP**. If you continue installation with a new passphrase, you will be unable to access your existing data

   **Confirm Passphrase** You cannot continue until the contents of this field are identical to the passphrase entered above.
5. In the **Destination Folder** window, review the location. If necessary, click **Change** to change the location where you want the Database Server component to be installed.
6. Click **Install.**

   To upgrade your database now, ensure that the **Launch Management Portal: Database Install Tool** check box is checked before clicking **Finish**.

   **Note:** This process does not install a new database. It installs the Database Installation Tool, which is used to set up the database.

   To set up your database, ensure that the **Launch Management Portal: Database Install Tool** check box is checked before clicking **Finish**.

If you checked the **Launch Management Portal: Database Install Tool** check box after installing the Database component, the database install tool launches

automatically. You can also launch the database install tool manually from **Start > All Programs > Management Portal > Database > Database Installer.**

The wizard will guide you through the process of installing a database.

Click **Next** to go through each window in turn. Enter the following details:

1. In the SQL Server Connection Details window:
   - **Server Name** Select the Microsoft SQL Server where the Unified CCMP database must be installed. 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 will be used for Unified CCMP. Use the default name of **Portal.**
   - **Connect Using** Select the radio button of the login credentials you want to apply:
     - 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** Make sure the connection to the Microsoft SQL Server is established. The message 'Connection succeeded but database does not exist' is correct behavior at this point. Click **OK** to continue.
2. In **Select an Action to Perform** window select **Install a new database**.
3. In the **Setup Replication** window for the Side A database server leave the Replicated Configuration checkbox unchecked and click **Next.**

   When installing the database on the Side B database server:
   - **Replicated Configuration** Check this box when installing the database on the Side B database server. The Share Name and Folder Path text boxes will become active
   - **Share Name** Enter the name of the share for the ReplData folder. By default this is **ReplData.**
   - **Folder Path** Enter the path of the ReplData folder. This is configured in Microsoft SQL Server. By default, it is **C:\Program Files (x86)\Microsoft SQL Server\MSSQL.1\MSSQL\repldata.**
4. The fields on the **Configure the Location of Data Files** window only need to be amended if you want to customize the size and location of the database files, otherwise click **Next.**
5. The **Configure SQL Server Agent Service Identity** window sets up a user account that is used by Microsoft 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 user account. This defaults to **sql_agent_user**. If you used a different name when setting up the account, enter that name instead. For a domain user include the domain

information so the name is of the form <DOMAIN>\sql_agent_user. For example if the SQL agent user belongs to the UCCMPDOM domain then enter UCCMPDOM\sql_agent_user.

- **Automatically create the user account if missing** For a single-sided system, it is possible to create the required user automatically. *For all other systems, you must set up the required account manually*. If you have not already created the user account, set it up now before continuing.
- **Password** Enter the password of the sql_agent_user account.
- **Confirm Password** You are unable to continue until the contents of this field are identical to the passphrase entered above.

6. In the **Web Application Servers Network Service Configuration** window, enter the details of each Web Server, from both sides, to be used in the installation:
   - **Domain** The network domain the web server resides; for example, UCCMPDOM.
   - **Machine Name** The name of the machine; for example, WEBSERVERA.

     **Note:** The database installer will use this information to grant access for the Network Service accounts on these web servers to the Portal database. If you need to add a new Web Server after the database has been installed you will need to grant permissions manually. For information on how to add these permissions manually, refer to chapter 9, Troubleshooting in the Unified CCMP Installation Guide for details.
7. Click **Add** to add each Web Server to the list.
8. When all Web Servers have been added, click **Next** to begin installation. Installation will take several minutes.
9. Click **Close** to close the installer.

For dual-sided systems repeat the database installation procedure on the Side B database server.

### Granting the Reporting Services Execution Account Permissions on the Unified CCMP Database

When upgrading a two-tier Unified CCMP deployment, permissions must be granted on the Unified CCMP database for the Reporting Services execution account. This is achieved by performing the following steps in the on all database servers after Unified CCMP Database Installation has been completed:

1. Select **Start > All Programs > Microsoft SQL Server 2005 > SQL Server Management Studio**. The SQL Server Management Studio displays.
2. Enter the credentials of the database server and click **Connect**.
3. Expand **Security > Logins** folder. Right-click **Logins** folder and select **New Login**. The Login – New window displays.

4. Enter the Login name: of the Reporting Services execution account user. This will be in the <DOMAIN>\<Username> form.
5. Select **User Mapping** option in the left of the window. The User Mapping information for the execution user displays.
6. The following configuration must be applied in this window:
    - Select the checkbox in the **Map** column next to the **Portal** database.
    - Whilst the Portal database is selected check the following checkboxes in the **Database role membership for: Portal** section of the screen:
        - portalapp_role
        - portalreporting_role
        - portalrs_role

    Click **OK** to save the new permissions and **Close**.

### Restoring the Portal Database Backup

Now that the Unified CCMP 8.5(2) database is installed, the backup of the existing Portal database can be restored.

The Portal databases must now be restored from the backups made earlier.

On the new Side A database server:

1. Click **Start > All Programs > Microsoft SQL Server 2005> Management Studio**.
2. Right Click the Portal database and Click **Tasks > Restore**.
3. In the Restore Database window choose **From Device** and **Add** the location of the portal back up file from the same side database server. You may need to copy the backup file locally in order to access it.
4. Select the backup file to restore the Portal database from and click **OK**.
5. Select the check box next to the backup set you just added
6. Select the Portal database as the restore destination from the **To Database** drop-down list.
7. Select **Options** and choose **Overwrite the existing database**.
8. Click **OK** to start the restore.

For dual-sided systems repeat the process on Side B to restore the Side B portal database backup to the new Side B database server.

Once the Portal databases have been restored they must then be upgraded.

### Upgrading the Portal Databases

The Portal databases must be upgraded to bring them up to the required version to operate correctly with Unified CCMP 8.5(2).

On the Side A Database Server:

1. If you checked the **Launch Management Portal: Database Install Tool** check box after installing the Database component, the database install tool

launches automatically, alternatively, click **Start > All Programs > Management Portal > Database > Database Installer.** The Database Installer Wizard Displays. Click **Next** to go through each window in turn

2. In the SQL Server Connection Details window:
   - **Server Name** Select the Microsoft SQL Server where the Unified CCMP database is installed. 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 is used for Unified CCMP (**Portal).**
   - **Connect Using** Select the radio button of the login credentials you want to apply:
     - The Windows account information you use to logon 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** Make sure the connection to the Microsoft SQL Server is established. Click **OK** to continue.
3. In **Select an Action to Perform** window:
   - Select **Upgrade an existing database**. Click **Next.**
4. In the **Select Source Media** window accept the defaults and click **Next**.
5. Click **Next** to begin the upgrade. The upgrade will take several minutes.
6. When the upgrade completes, click **Close** to close the Database Installer Wizard.

The Portal database is now upgraded.

For a dual-sided system repeat the process on the Side B database server to upgrade the Side B Portal database.

Once the Portal database is upgraded, the remaining Unified CCMP components can be installed.

**Caution:** When prompted for the cryptographical password during the installation of you must use the password used during the initial installation of Unified CCMP.

### Application Server Component

Install the Application Server Component as described in the Application Server Component section in Chapter 4. When prompted for the cryptographical passphrase, enter the passphrase you created during installation of the Database Server component **when you first installed CCMP**.

### Web Server Component

Install the Web Server Component as described in the Web Server Component section in Chapter 4.

### Data Import Server Component

Install the Data Import Server Component as described in the Data Import Server Component section in Chapter 4. When prompted for the cryptographical passphrase, enter the passphrase you created during installation of the Database Server component **when you first installed CCMP**.

### Provisioning Server Component

Install the Provisioning Server Component as described in the Provisioning Server Component section in Chapter 4. When prompted for the cryptographical passphrase, enter the passphrase you created during installation of the Database Server component **when you first installed CCMP**.

For dual-sided systems, repeat the installation of each component on the Side B servers.

After the Unified CCMP components have been installed the upgraded Unified CCMP environment may be configured.

## Unified CCMP Configuration

After the database has been upgraded and the Unified CCMP 8.5(2) components have been installed, the following configuration updates must be made.

### Add the Application Servers to the Cluster

Depending on the version of Unified CCMP you are upgrading from, you may need to re add the Application Servers into the Unified CCMP cluster.

On the Side A database server:

1. Click **Start > All Programs > Management Portal > Configuration Manager**. The Configuration Manager tool displays.
2. Click **OK** to connect to the local Portal database.
3. Click **UCCMP Servers**. The Application Servers tab is displayed. In the left of the window is a list of servers in the cluster. The right hand panels should display which of the servers are the primary and in the case of a dual-sided system, secondary, application servers. If the panels on the right do not show the application servers, perform the following steps to add the application servers.
    a. In the Available Servers list, check the server which is the Side A Web Server.
    b. Use the arrow button to move it to the **Primary Application Servers** list.
    c. If there is a Side B Web Application Server, check the **Dual-sided** check box. Select the server which is to be the Side B Web Server and move it to the **Secondary Application Servers** list.

Remain in the Configuration Manager tool. If you are upgrading a dual-sided system proceed to Re instantiating Portal Database Replication otherwise proceed to Add the Report Server Databases to the Cluster.

### Re instantiating Portal Database Replication

To re instantiate replication perform the following steps.

1. In Configuration Manager on the Side A database server click the **UCCMP Databases** tab in the UCCMP Servers section of Configuration Manager. A table displays with four columns that contain information about the configured databases.
2. Click **Replication.** The UCCMP Database Replication Configuration window opens and displays all the selected server details. Perform any modifications at this stage if necessary.

   **Note:** The path values for the data files and log files will reflect those for the pre upgrade database as the database restore will have overwritten the new values. Ensure that these values are changed to match the current location of the Portal database data files and log files.

3. Click **Replicate** (if asked to save changes, click **Yes**) and confirm. This will open a work execution window that will show the progress statuses for replication.
4. To start the replication configuration process click **Execute**. When asked to confirm replication, click **Yes**. After the replication is set up successfully click **Close**.
5. Click **OK** to close the UCCMP Database Replication Configuration window.
6. Click **Close** to close the UCCMP Configuration Window**.**
7. Log in to the Side B database server (the subscriber) and open the **SQL Server Management Studio**.
8. Right click the Replication folder then click **Launch Replication Monitor**. The Replication Monitor displays.
9. Expand **My Publishers**. If the Side A database server publisher is not shown then it must be added:
   a. Right click **My Publishers > Add Publishers.** The Add Publisher dialog box displays.
   b. Click **Add > Add SQL Server Publisher**.
      - **Server Name** Enter the name of the Side A (publisher) server.
      - **Authentication** Enter authentication details to connect to the server.
10. Click **Connect**. If a notification message about the distributor location is displayed, click **OK** and provide connection details for the distributor.
11. Click **OK** to add the publisher to the list of monitored publishers.
12. Navigate to the snapshots listed below the Publisher. Two snapshots display called:
    - [Portal] Base
    - [Portal] NonQueued
13. Click on the base publication snapshot and then click on the **Warnings and Agents** tab.

14. Right click on the Snapshot Agent in the Agents and Jobs list and click **Start Agent.** Wait for the status to change to 'Completed'. This may take several minutes.
15. Repeat steps 12 and 13 for the Non Queued snapshot.
16. Exit the Replication Monitor and close SQL Server Management Studio.

Unified CCMP database replication setup is now complete.

Proceed to the next section to configure and replicate the Reporting Services databases.

### Add the Report Server Databases to the Cluster

Depending on the version you are upgrading from you may need to add the report server databases into the Configuration Manager.

On the Side A database server:

1. Click the **Report Server Databases** tab.
2. If the Report Server databases are not shown, click **New.** The Report Server Database Configuration dialog box displays.
   a. **Server** Choose the Side A database server.
   b. **Authentication C**hoose windows authentication.
3. Click **OK**.

For a dual-sided CCMP installation, remain in the Configuration Manager tool and repeat steps 2 and 3 adding the Side B report server database then proceed to the next section to set up Reporting Services replication.

For a single sided CCMP installation save and exit the Configuration Manager and follow the steps in Chapter 6, Post-Installation Steps.

### Report Server Database Replication

For a dual-sided Unified CCMP installation the Configuration Manager tool allows you to replicate Report Server databases. This is required for dual-sided configurations of Unified CCMP.

1. Click **Replication** on the Report Server Databases tab of Configuration Manager. The Report Server Database Replication Configuration window displays.
2. Click **Replicate;** if asked to save pending changes, click **Yes**.
3. To start the replication configuration process click **Execute**.
4. You will be asked to take a backup of the report server encryption key from the Publisher before setting up replication.
5. To *back up* the report server encryption key do the following:
   a. Log in to the Side A web server.
   b. Click **All Programs > Microsoft SQL Server 2005 > Configuration Tools > Reporting Services Configuration**. The Reporting Services Configuration Manager displays.

c. In the Instance Selection window, select the Side A Report Server and click **Connect**.

d. Click **Encryption Keys**. The Encryption Key window displays to the right.

e. Click **Backup**.

f. Enter a password.

g. Click **…** (to the right of Key File).

h. Enter a File name; make a note of it for future reference (this will have the **.snk** extension file name).

i. Click **Save**.

j. **Exit** the Reporting Services Configuration tool.

6. Return to the Report Server Database Replication Manager.
7. Confirm that you have backed up the report server encryption key.
8. If replication is successful, you will see a message in the Report Server Database Replication Manager window saying you should restore the encryption key from the publisher report server to the subscriber report server.
9. To *restore* the report server encryption key on the subscriber do the following:

   a. Log in to the Side B web server.

   b. Click **All Programs > Microsoft SQL Server 2005 > Configuration Tools > Reporting Services Configuration**. The Reporting Services Configuration Manager displays.

   c. In Instance Selection window, select the Subscriber and click **Connect**.

   d. Click **Encryption Keys**. The Encryption Key window displays to the right.

   e. Click **Restore**.

   f. Enter the password.

   g. Click **…** (to the right of Key File).

   h. Locate the **.snk** file containing the encryption key.

   i. Click **Open**.

   j. Click **OK**. The restoration of the encryption key is complete.

   k. **Exit** the Reporting Services Configuration tool.

10. Return to the Report Server Databases tab and Exit the Configuration Manager.

Reporting Services configuration is now complete.

### Configuring the Windows firewall for UCCE Provisioning

**Note:** By default the Windows Server 2008 R2 Firewall will not allow incoming traffic for Unified CCMP. If the Windows firewall is on create a rule to allow inbound TCP traffic for Unified CCMP to communicate with each configured UCCE.

This should be done for the Local Registry Port and Local Port stored for each Unified ICM server stored in the Unified CCMP Configuration Manager.

Steps for adding a firewall rule are described in the Configuring Windows 2008 R2 Firewall for SQL Server section of Chapter 3.

The Unified CCMP upgrade is now complete. Exit the configuration manager and follow the steps in Chapter 6, Post-Installation Steps, to start the Unified CCMP services, login to Unified CCMP and upload the Unified CCMP audit reports.

# 8. Platform Uninstallation

This chapter describes how to remove the Unified CCMP 8.5(2) platform components. The uninstallation procedure must be performed in the following order.

## Uninstalling the Data Import Server and Provisioning Components

This process removes the Data Import Server and Provisioning Server components.

### Removing Replication

**If you have a dual-sided installation, follow these steps to remove replication before uninstalling the Data Import Server.**

First, you must stop the **UCCMP: Data Import Server** service. To do this, proceed as follows:

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

You may now remove replication.

Follow these steps to remove replication from the Portal databases.

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. Click **Start > All Programs > Management Portal > Configuration Manager**.
3. Click **UCCMP Servers**.
4. Select the **UCCMP Database** tab.
5. Click **Replication**.
6. Click **Unreplicate**.
7. Click **Yes** when prompted to remove replication

**Note** Removing replication may take some time.

After replication has been successfully removed then you may close the Configuration Manager and proceed to remove the Data Import Server component.

### Uninstalling the Data Import Server Component

This process will remove the Data Import Server Component.

1. On the Side A database server, click **Start > Control Panel > Uninstall a Program**. The Programs and Features window displays.
2. Select **Management Portal: Data Import Server**.
3. Click **Uninstall**. A window displays asking you if you are sure that you want to remove the Management Portal: Data Import Server.
4. Click **Yes**. The Setup Status window displays. The extent of the uninstallation progress displays on the progress bar.

For dual-sided installations, repeat this process on the Side B database server.

### Uninstalling the Provisioning Server Component

This process will remove the Provisioning Server component, removing Unified CCMP connection for any remote data sources, such as Unified ICM or Unified CM.

1. On the Side A database server, click **Start > Control Panel > Uninstall a Program**. The Programs and Features window displays.
2. Select **Management Portal: Provisioning Server**.
3. Click **Uninstall.** A window displays asking you if you are sure that you want to remove the Management Portal: Provisioning Server.
4. Click **Yes**. The Setup Status window displays. The extent of the uninstallation progress displays on the progress bar.
5. When the uninstallation completes, restart the system. If you are upgrading a single-tier system, the reboot will cause the remaining Unified CCMP services to start. Repeat the steps from earlier in the process to stop them.
6. Manually delete the folder: **C:\Program Files\Management Portal\Provisioning Server\Config** if it exists.

For dual-sided installations, repeat this process on the Side B database server.

## Uninstalling the Database Component

This process removes the database installation component and Unified CCMP database catalogs**. Do not remove the database catalogs from your system unless you intend to permanently remove Unified CCMP.**

**Caution** If upgrading an existing version of the Unified CCMP, *DO NOT* perform this step because it will remove all your existing data.

1. On the Side A database server click **Start > All Programs > Management Portal > Database > Database Installer**. The Database Setup window displays.
2. Click **Next.**
3. In the SQL Server Connection Details window:
   - **Server Name** Select the Microsoft SQL Server where the Unified CCMP database is installed. 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 is used for Unified CCMP (**Portal).**
- **Connect Using** Select the radio button of the login credentials you want to apply:
  - 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** Make sure the connection to the Microsoft SQL Server is established. Click **OK** to continue.

4. In the **Select an Action to Perform** window select **Delete an existing database**. Click **Next.**
5. Click **Next** to remove the database.
6. When the deletion of the database completes, click **Close** to close the Database Installer Wizard.

After the Portal database has been deleted the Database Installer tool can be removed:

1. On the Side A database server, click **Start** > **Control Panel** > **Add or Remove Programs**. The **Add/Remove Programs** list displays.
2. Select **Management Portal: Database Install Tool.**
3. Click the **Remove** option, and confirm.

For dual-sided installations, repeat this process on the Side B database server.

## Uninstalling All Other Components

All other components can be uninstalled by clicking **Uninstall** from the **Programs and Features** window. Uninstall them in the following order:

1. Management Portal: Language Pack
2. Management Portal: Web Application (Web Server component)
3. Management Portal: Application Server (Application Server component)

**Note:** In some circumstances, uninstallation may not be able to stop Microsoft Reporting Services in a timely fashion. If an error occurs during uninstallation, use the **services.msc** command to check that the **ReportServer** service is stopped. Then reattempt uninstallation. After uninstallation is complete, restart the **ReportServer** service.

# 9. Troubleshooting

## Installing Unified CCMP Components with Logging Enabled

Unified CCMP installers can be launched with logging enabled to assist with troubleshooting installation issues. To install the Unified CCMP components with logging enabled, perform the following:

1. At the command prompt navigate to the directory containing the component installation files.
2. Execute **setup.msi /lv*** <logfile> (where <logfile> is the path and name of the file that will contain the debug output). For example:

   ```
   setup.msi /lv* c:\mylog.txt
   ```

   Will output debug information to the file `c:\mylog.txt`
3. Install Shield Wizard opens for the selected component, click **Next** to continue the installation as described in Chapter 4, Component Installation.

This method can be applied to all Unified CCMP components.

## Adding a New Web Server After the Database Is Installed

In the event of system recovery or system expansion a new web server may need to be installed. Under normal installation conditions the details of the web server are known at install time and can be provided during the database installation so that suitable permissions for access to the database from the web server's Network Service account can be applied by the installer. Adding a web server to the cluster at a later date requires permissions to be set up manually in Reporting Services and for permissions to be granted for the Web Server's Network Service Account on the Portal database. To set up Reporting Services permissions for the new Web Server:

1. Log in to the Web Server.
2. Navigate using Internet Explorer to the following URL: **http://localhost/reports**. The Reporting Services Report Manager screen displays.
3. Select the **Properties** tab. The Properties tab displays with the Security section open.
4. Select **New Role Assignment**. The New Role Assignment window displays.
5. Set a new Network Service account in place of the standard NT Authority\Network Service account for this web server in **Group or user name**. Enter the name of the machine in the `<DOMAIN>\<MACHINENAME$>` form. For example, for a machine called CCMPWEBBC on the CISCO domain enter `CISCO\CCMPWEBBC$`.
6. Select the following **Roles** from the list:
   - Browser
   - Content Manager
   - My Reports

- Publisher
- Report Builder

7. Click **OK** to add the new role assignment. The Security section of the Properties tab displays showing the newly added User Role Assignment.
8. Select the **Site Settings** link at the top of the page. The Site Settings window displays.
9. Select the **Configure site-wide security** link. The System Role Assignments window displays.
10. Select **New Role Assignment**. The New Role Assignment window displays.
11. Add the network service account for the new Web Server in **Group or user name**.
12. Choose the following Roles from the list:
    - System Administrator
    - System User
13. Click **OK** to add the new role assignment. The System Role Assignments window displays.
14. Click **Exit** to close the Reporting Services Configuration Manager.

To add permissions for the new Web Server's Network Service Account on the Portal database:

1. Using the **SQL Server Management Studio** connect to the Portal database, right-click on the **Security** folder beneath the server instance in the **Object Explorer** pane and select **New > Login**.
2. Enter the name of the machine in the **Login Name** field in the `<DOMAIN>\<MACHINENAME$>` form.
3. Click **OK**.
4. Right-click on the **Security** folder beneath the Portal database and select **New > User**.
5. Enter the name of the machine in the **User Name** field in the `<DOMAIN>\<MACHINENAME$>` form.
6. Enter the name of the login created in Step 2 in the **Login Name** field or select it using the Explore dialog box.
7. Select the following roles in the **Database Role Membership** list:
    - db_datareader
    - db_datawriter
    - db_ddladmin
    - db_securityadmin
    - portalapp_role
    - portalreporting_role
    - portalrs_role

8. Click **OK.**

# Upgrade Troubleshooting

This section describes troubleshooting and resolution steps for common issues encountered when performing an upgrade.

## SQL Server 2005 Reporting Services Upgrade Troubleshooting

When upgrading from SQL Server 2000 to SQL Server 2005 Reporting Services issues can arise when configuring Reporting Services following the upgrade.

### Reporting Services Database Upgrade Fails

When upgrading the Reporting Services database from SQL Server 2000 to SQL Server 2005 the upgrade can fail because database roles that are required by SQL Server 2005 Reporting Services are not present on the restored SQL Server 2000 database.

In this situation the upgrade will fail with the following message:

> There was a problem applying the database upgrade script.

The **Tell me more** link provides the following additional detail:

> System.Data.SqlClient.SqlException: Cannot find the user 'RSExecRole', because it does not exist or you do not have permission.

To work around this issue it is necessary to create a new Reporting Services database to create the required roles and then switch back to the original database to perform the upgrade. In the Reporting Services Configuration Tool Database Setup screen, perform the following steps:

1. Enter the name of the database server in **Server Name**.
2. Click **Connect** and **OK** to connect to the database.
3. Click **New**. The SQL Server Connection dialog box is displayed.
4. Enter the name for a new ReportServer database in **Database Name**. This database will not be used by Unified CCMP so use a different name to the original Unified CCMP ReportServer database such as ReportServer2.
5. Click **OK** to create the database.
6. When the database has been created and you have been returned to the Database Setup screen, change the **Database Name** back to the name of the original ReportServer database; by default this is ReportServer.
7. Click **Upgrade** and **OK** to upgrade the database.
8. Click **Apply** and **OK** to apply the new database.

Configuration of the Report Server can now be resumed.

### Reports Do Not Run After the ReportServer Database Is Upgraded

When upgrading from SQL Server 2000 to SQL Server 2005 Reporting Services issues can arise when running a report following the upgrade.

If this issue occurs the following error is displayed when attempting to run the report:

An internal error occurred on the report server. See the error log for more details. (rsInternalError)

Cannot insert the value NULL into column “SnapshotDataID”, table “ReportServerTempDB.dbo.SessionData”; column does not allow nulls. INSERT fails. The statement has been terminated.

The ReportServerTempDB database schema must be updated to correct this issue.

Steps for resolving this can be found at: http://support.microsoft.com/kb/946741.

**Note:** The resolution steps for this issue require that the Reporting Services database is not replicated. If you need to apply these steps after replicating the Reporting Services database, first remove Report Server database replication using the Unified CCMP Configuration Manager. Replication can be reapplied after the resolution steps are applied.

# Glossary

## A

**Audit**

A diagnostic process instigated to assess system performance.

## C

**Certificate**

A digital certificate is a means of establishing your credentials when performing transactions over the Internet. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

**Cluster**

Multiple networked servers, which form the platform across which Unified CCMP is deployed.

**Commissioning**

Any action or process required to set up the Unified CCMP platform that is not set up by the Unified CCMP installer or inherent tools.

**Configuration**

The hardware and/or software components that comprise a system and the manner in which they are connected.

**Connection**

The link between two nodes in a script or between a node and a routing target set. Connections show the flow of control between objects in the script. Within the Script Editor, a connection is represented as a line segment.

**Connectors**

Connectors consist of:

- Telephony connectors that Unified CCMP uses to interface with routing components during call routing.
- Business connectors that Unified CCMP uses to interface with back office databases to collect data that is used to determine the route of the call or that is to be packaged with the call to inform the contact center agent

## D

**Domain**

In the Internet, domains are defined by the IP address. All the networked computers and devices sharing a common part of the IP address belong to the same domain. They are administered as a whole unit with the same rules and procedures.

## F

**Failover**

A back up process used when the primary process fails.

**Field**

A space in a database allocated to an item of information. A collection of fields is called a record.

**Firewall**

A security measure placed between trusted and un-trusted sites. It filters out traffic that can damage the host network or connected hardware.

## H

**Hyper Text Transfer Protocol (HTTP)**

The protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted and the actions Web servers and browsers are to take in response to commands.

**HTTPS - (HTTP) + Secure Sockets Layer (SSL)**

This is a secure version of the Hyper Text Transfer Protocol as it includes the Secure Sockets Layer (SSL), which is a layer of encryption added to data requests from an HTTP server.

## M

**Map**

A map is used to logically connect two entities. As programs cannot translate directly from human concepts to computer numbers, the concepts are translated incrementally through a series of layers. Each layer contains the same amount of information as the layer above but in a closer form to that which the computer understands. This process of translating from one layer to another is called mapping.

**Microsoft SQL Server**

The Microsoft relational database product used for the Unified ICM local and central databases.

## P

**Portal User**

Someone who has access to the user interface, their level of access will depend on the settings allocated to them by the System Administrator.

**Power User**

Someone who can access functionality above that of a basic user, for example a Supervisor.

## R

**Report**

The means by which Unified CCMP provides to a user information about what is occurring within the system itself. An example would be an audit report, which shows what changes have been performed on the contact center's resources.

## S

**Secure Sockets Layer (SSL)** – (See (HTTP) + Secure Sockets Layer (SSL))

**Service Provider**

A business that provides a service to another business, for example a telecommunications network.

**Structured Query Language (SQL)**

A database query language in which statements are formulated to manipulate or request data in a database.

**String**

A series of characters that have been arranged into a specific grouping in a coded script.

## T

**Tenant User**

The Tenant User is a user who only has access to the resources and tools assigned to them by the Tenant Administrator. Several sub-classes of tenant user can be created by the Tenant Administrator using user groups and roles to achieve business requirements.

## U

**Uniform Resource Locator (URL)**

The global address of documents and other resources on the World Wide Web. The first part of the address indicates the protocol to use, and the second part specifies the IP address or the domain name where the resource is located.

## W

**Web Browser**

A software application used to locate and display Web pages.

# Index


***A***

AJAX Extensions....5, 6
Application Instance List....35
Application Key....23, 35, 43, 45
Architecture....3
Audit....50
Audit Reporting....50
autorun.hta....6

***C***

CMS Server....35
cms_jserver....35
cmsnode....35
ConAPI....33, 34, 36, 43, 45, 47
Cryptography....25, 28, 30, 31, 63
CVP Media File Upload....50

***D***

Deployment Models....3
Deployment Specifics....2
DFS Root Targets....51
Diagnostic Framework....31, 32
Distributed File System....51
Domain User Accounts....9

***F***

FIPS compliance....8
Firewall....17, 71, 72, 81

***J***

J2SE Runtime Environment....5, 6

***L***

Languages....52
Local Port....43, 72
Local Registry Port....23, 43, 45, 72

***M***

Microsoft SQL Server 2005 SMO 5, 6
Mixed Mode....12, 16

***N***

NAM....44
NET Framework 3.5....5, 6, 8, 9
Network VRU Script....50

***P***

PG User....47
Prerequisites....5, 6

***R***

Remote Registry Port....43, 45
Report Server Databases....40
  Replication....40
report_execution_user....9
Reporting Services Execution Account....14
Resilience....3

***S***

Security Hardening....55
Single Tier....3
SQL Native Client Configuration....13, 17
SQL Server Service Pack....6, 10
sql_agent_user....9, 23, 27, 64, 65

***T***

Tenant Administrator....1, 82
Tenant Supervisor....1
Two Tier....3

***U***

UCCMP Database....38
  Replication....38
Unified CM....46
Unified ICM....42
Upgrade....56, 58

***W***

WAV....50
Windows Authentication....12, 16, 34, 37
WSE 2.0 SP3....5, 6