Installation and Configuration Guide for Cisco Unified Contact Center Management Portal

Release 11.0(1)

August 2015

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

Table of Contents

Preface

Purpose

This document explains how to install the 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) system architecture. Microsoft SQL Server database administration experience is also helpful.

Organization

The sections of this guide are as follows:

Chapter 1	Planning Your Installation	Introduces Unified CCMP, including its integration with Unified CCE.
Chapter 2	Installation Requirements	Lists the prerequisites for Unified CCMP installation and provides recommendations for pre installation platform configuration.
Chapter 3	Windows and SQL Installation and Configuration	Describes how to setup the Microsoft SQL Server.
Chapter 4	Unified CCMP Installation	Provides instructions for the installation of all Unified CCMP components.
Chapter 5	Unified CCMP Configuration	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 Replication Manager to replicate data between Database Servers. Web and Database component server performance checklists are also provided.

Chapter 6	Post-Installation Steps	Describes the post-installation options and the system checks for the Unified CCMP platform.
Chapter 7	Upgrading From a Previous Version	Explains the various options for upgrading an existing installation of Unified CCMP without losing your data.
Chapter 8	Single-Sided Upgrade	Describes how to upgrade a single-sided deployment.
Chapter 9	Total Outage Upgrade	Describes how to upgrade a dual-sided deployment in one operation.
Chapter 10	Split Sided Upgrade	Describes how to upgrade a dual-sided deployment in two stages, one side at a time.
Chapter 11	Uninstalling Unified CCMP	Describes how to remove Unified CCMP from your servers.
Chapter 12	Troubleshooting	Describes how to enable logging for the Unified CCMP Installer and how to apply database permissions after the Installer has completed.

Document Conventions

This document uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as entries, keys, buttons, folders and submenu names. For example: • Choose **Edit > Find** • Click **Finish**
italic font	Italic font is used to indicate the following: • To introduce a new term; for example: A *skill group* is a collection of agents who share similar skills • For emphasis; for example: *Do not* use the numerical naming convention • A syntax value that the user must replace; for example: IF (*condition, true-value, false-value*) • A title of a publication; for example: Refer to the *Cisco CRS Installation Guide*

Convention	Description
window font	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays; for example: `<html><title>Cisco Systems, Inc. </title></html>`
< >	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output • A character string that the user enters but that does not appear on the window, such as a password

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Field Alerts and Field Notices

Cisco products may be modified or key processes may be determined to be important. These are announced through use of the Cisco Field Alerts and Cisco Field Notices. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

Log into www.cisco.com and then access the tool at http://www.cisco.com/cisco/support/notifications.html

Documentation Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

1   Planning Your Installation

1.1   About Your Installation

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

1.2   Deployment Specifics

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

Each configured Unified CCE instance must have its own:

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

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

1.3   Infrastructure Software

Unified CCMP requires:

*   Windows 2012 Server R2
*   SQL Server 2014 64-Bit Standard Edition.

1.4   Unified CCMP Components

A Unified CCMP installation comprises the following components.

- the **Database Server**, which holds information about resources (such as agents, skill groups and dialed numbers) and actions (such as phone calls and agent state changes) in the system. It consists of:

  - the **Portal Database** , which holds the data that has been provisioned through Unified CCMP or imported from Unified CCE

  - the **Data Import Server**, which imports and synchronizes resources and changes to resources from back-end contact center systems (for example, Unified CCE)

  - the **Provisioning Server**, which applies resource changes made by Unified CCMP users to the back-end contact center systems

  - the **Partitioning Server**, which manages the creation and removal of Unified CCMP partition tables, used to store contact center data

- the **App/Web Server** which provides two components for interfacing with Unified CCMP:

  - **Application Server** delivers application services such as search, security and resilience to the Unified CCMP Web Server

  - **Web Server** provides the web front end that allows users perform resource management and administrative tasks.

1.5   Deployment Models

In many environments, Unified 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 App/Web 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.

- **Two Tier (Secure Deployment)**. Unified CCMP Application and Web components are hosted on one server. The Provisioning, Data Import and Database components are hosted on a second server.

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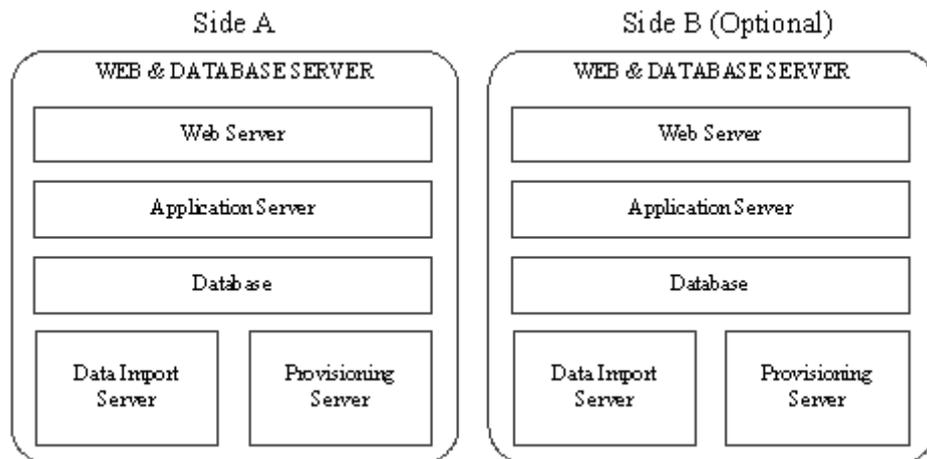
Figure 1.1   Component Layout for a Single Tier Deployment

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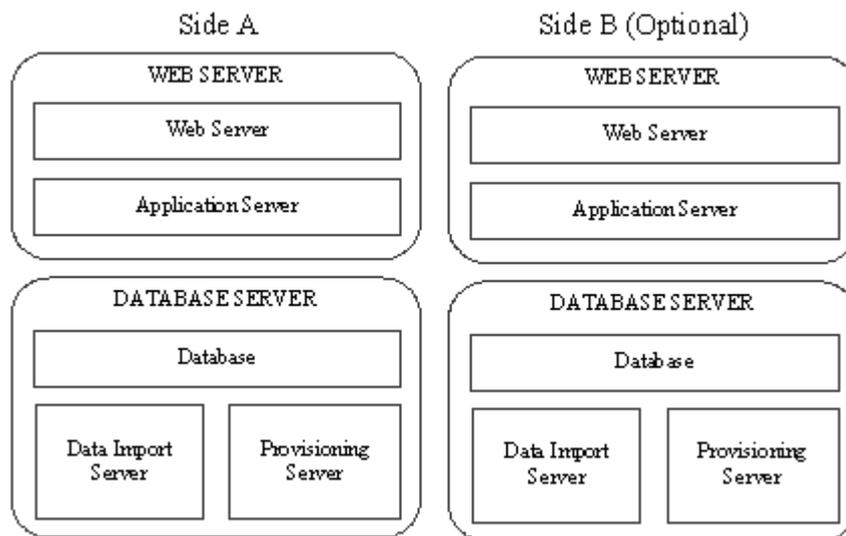
Figure 1.2   Component Layout for a Dual Tier Deployment

2   Installation Requirements

2.1   Installation Prerequisites

2.1.1   About the Installation Prerequisites

This section describes the installation prerequisite requirements for Unified CCMP.

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

2.1.2   General Requirements

This section describes the general requirements for your installation.

- Do not install any Unified CCMP component on a domain controller.
- Unified CCMP server names must consist of alphanumeric characters only, without underscores or hyphens.
- Your system infrastructure and domain controller must be configured to handle IPv6 configured servers and addresses.
- All app/web servers must be configured to support IPv4 addressing for internal component communication, and IPv6 addressing for handling web traffic.
- All other Unified CCMP servers must have an IPv4 address only.
- Unified CCMP does not support SQL Server named instances. All SQL Server installations must use the default instance name.
- It is recommended that the SQL Server **TempDB** directory and **TempDB** log directory are not located on the same disk as the operating system.

2.1.3   System Requirements

Ensure these requirements are satisfied before starting the installation.

- All Unified CCMP servers require Windows Server 2012 R2.

2.1.4   Additional Software Requirements

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

The Unified CCMP servers that require SQL Server must meet the installation prerequisites defined in https://msdn.microsoft.com/en-US/library/ms143506 (v=sql.120).aspx (link checked July 2015).

2.1.4.1   Database Servers

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

- Microsoft SQL Server 2014 64 bit Standard Edition
- Microsoft SQL Server 2014 64 bit Workstation Components

2.1.4.2   App/Web Servers

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

2.1.5   Clients running the Web Application

The Unified CCMP web application supports the following browsers:

- Internet Explorer versions 8 to 11 (although some gadgets require version 9 or later, for example, the Charts gadget).
- Google Chrome versions 25 to 36.
- Mozilla Firefox versions 18 to 31.

2.2   Firewall Configuration

2.2.1   About Firewall Configuration

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

The Windows firewall must be configured to allow the various components of Unified CCMP to communicate with one another in a distributed environment. It is recommended that port restrictions are limited to only the servers that require the specified communications channels.

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

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

Note

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

2.2.2   Web Server Port Usage

Note

The ports listed in this table must be configured to accept traffic from IPv6 addresses.

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

2.2.3   Unified CCMP Database Server Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Servers Requiring Access	Usage
SQL Server	TCP	1433	Other Database Servers, Application Servers	General
DTC	TCP	2103	Other Database Servers	Audit Archive
DTC	TCP	2105	Other Database Servers	Audit Archive
DTC (RPC)	TCP	135	Other Database Servers	Audit Archive
DTC (RPC)	TCP	5000-5100*	Other Database Servers	Audit Archive

Application Protocol/Service	Protocol	Incoming Ports	Servers Requiring Access	Usage
NetBIOS File Share	UDP	137-138	Other Database Servers, Application Servers	Replication, Unified CVP File Upload
NetBIOS File Share	TCP	139	Other Database Servers, Application Servers	Replication, Unified CVP File Upload
SMB (DFS)	TCP	445	Other Database Servers, Application Servers	Unified CVP File Upload File**
ConAPI Local Registry	TCP	2099***	Unified CCE Admin Workstation	Provisioning
ConAPI Local Port	TCP	3333***	Unified CCE Admin Workstation	Provisioning
ConAPI Local Port	TCP	3334****	Unified CCE Admin Workstation	Provisioning (Dual-sided deployments only)

* Dynamically assigned RPC port range used by MSDTC. Configured in registry as:

    HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet

After each change the machine must be restarted.

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

*** Default value for Side A - configured in Cluster Configuration. Must be open on both sides of a dual-sided deployments.

**** Default value for Side B - configured in Cluster Configuration. Must be open on both sides of a dual-sided deployments. Not required for single sided deployments.

2.2.4   Cisco Unified CCE Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Servers Requiring Access	Usage
SQL Server	TCP	1433	Database Servers and Application Servers	Importing Dimension Data, Provisioning Activities.
ConAPI Remote Registry	TCP	2099*	Database Servers	Provisioning

Application Protocol/Service	Protocol	Incoming Ports	Servers Requiring Access	Usage
CMS Node	UDP	9000	Database Servers	Ping Port for ConAPI services
Web Service API	TCP	443	Database Servers	Provisioning

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

2.2.5 Domain Controllers for Unified CCE Instances Port Usage

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

2.2.6 Cisco Unified Communications Manager Port Usage

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

2.2.7 Cisco Unified CVP Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Servers Requiring Access	Usage
Operations Web Service API	TCP	443	Database Servers, Application Servers	Provisioning

2.2.8 Other Information

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

- Distributed Transaction Coordinator

- File and Printer Sharing.

2.3　Security Considerations

2.3.1　Mandatory Security Configuration

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

You must:

● Configure Secure Sockets Layer (SSL) for the Unified CCMP web application (see section 6.2 "Configure SSL" for instructions).

2.3.2　Optional Security Configuration

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

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

● Disable anonymous sessions on all Unified CCMP servers (see section 3.4.1 "Disable Anonymous Sessions" for instructions). This prevents anonymous users from enumerating usernames and shares, and from using this information to guess passwords or perform social engineering attacks. For more information, consult the Microsoft documentation http://technet.microsoft.com/en-us/library/dd349805(WS.10).aspx#BKMK_38 (link checked November 2014).

● Disable cached logins on all Unified CCMP servers (see section 3.4.2 "Disable Cached Logins" for instructions). This prevents attackers from accessing the cached login information and from using a brute force attack to determine user passwords. If cached logins are disabled, windows domain users will be unable to log in if the connection to the domain controller is unavailable. For more information, consult the Microsoft documentation http://technet.microsoft.com/en-us/library/dd349805(WS.10).aspx#BKMK_27 (link checked November 2014).

● Disable DCOM on all Unified CCMP servers (see section 3.4.3 "Disable DCOM" for instructions). This makes the server less attractive to malware, which may be used to gain elevated privileges and compromise the system. For more information, consult the Microsoft documentation http://technet.microsoft.com/en-us/library/dd632946.aspx (link checked November 2014).

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

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

- Disable SSL v2 on all App/Web Servers (see section 3.4.5 "Disable SSL V2" for instructions).This ensures that the latest security encryption technology and the most recent security fixes are being used.

3 Windows and SQL Installation and Configuration

3.1 Windows Configuration

3.1.1 Firewalls

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

3.1.2 All Unified CCMP Servers

1. On each of the Unified CCMP servers in your installation:

   - configure the server to use the US English character set

   - configure Microsoft Terminal Services for remote configuration and support

   - in the Event Viewer, set the Application Log, Security Log and System Log to **Overwrite events as needed**.

2. Using the Windows Time Service, ensure the date and time are synchronized across all Unified CCMP servers. Unified CCMP will not be able to synchronize application data correctly between servers otherwise, and this may cause unexpected behavior.

3.2 SQL Server

3.2.1 Install SQL Server

Follow these instructions to install SQL Server 2014 64-bit Standard Edition on the server or servers that will be hosting the Unified CCMP database.

On the Side A server:

1. In the SQL Server Installation Center, select **Installation**.

2. Select **New installation or add features to an existing installation**.

3. The **Setup Support Rules** window displays, validating the system for the SQL Server installation. Once validation passes click **OK**.

4. Enter the SQL Server product key and click **Next**.

5. Read the license terms. If you agree with the terms, select **I accept the license terms** and click **Next**.

6. You will be prompted to install the setup support files. Click **Install**.

7. Once the setup of support files is complete you will see a summary of checks. Review the results and make any necessary changes. If you see a warning saying that Windows Firewall is enabled, you can ignore it. When you are satisfied, click **Next**.

8. Select the **SQL Server Feature Installation** option and click **Next**.

9. Select the following instance features:

    - **Database Engine Services**
        - **SQL Server Replication**
    - **Client Tools Connectivity**
    - **Integration Services**
    - **Client Tools Backwards Compatibility**
    - **Management Tools – Basic**
        - **Management Tools – Complete**

10. Update the installation directories to the required locations. Click **Next**.

11. The installation rules are then checked. If any problems are reported, correct them, then click **Next**.

12. The **Instance Configuration** window is displayed. Select **Default Instance**, with an **Instance ID** of **MSSQLSERVER**. Update the Instance root directory to be installed on the required drive, then click **Next**.

13. The **Disk Space Requirements** summary window is displayed. Click **Next**.

14. In the **Server Configuration** window, on the **Service Accounts** tab, set the following service configuration:

    - Locate the **SQL Server Agent** entry in the **Service** column, and set the **Account Name** to **NT AUTHORITY\SYSTEM** and the **Startup Type** to **Automatic**.

- Locate the **SQL Server Database Engine** entry in the **Service** column and set the **Account Name** to **NT AUTHORITY\SYSTEM**.

15. In the **Server Configuration** window, on the **Collation** tab, ensure that the **Database Engine Collation** is **Latin1_General_CI_AS**. If it is not, click **Customize**, and select a collation designator of **Latin1_General**, ensure that **Case-sensitive** is cleared and **Accent-sensitive** is selected, then click **OK**. When the collation is correct, click **Next** to proceed.

16. The **Database Engine Configuration** window is displayed.

    - Select **Mixed Mode** authentication and enter a password for the **sa** user.

    - In the **Specify SQL Server Administrators** panel click the **Add Current User** button. Also add any other accounts that require administrator permissions to the database, for example, domain admins, service accounts etc.

    - Select the **Data Directories** tab. It is strongly recommended that **Temp DB directory** and **Temp DB log directory** are not located on the same drive as the Windows operating system. You will see a warning during Unified CCMP installation if they are. Make any required changes to the data directory locations.

    - Click **Next** to proceed.

17. You may see the **Feature Configuration Rules** window while installation checks are performed. If so, wait until the checks complete successfully.

18. Review the installation summary and click **Install**.

19. Once the installation is complete click **Close**.

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

3.2.2 Configure SQL Server Network Protocols

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

1. Launch **SQL Server 2014 Configuration Manager** to open the SQL Server Configuration Manager.

2. In the left hand pane, expand **SQL Server Network Configuration** and click **Protocols for MSSQLSERVER**.

3. In the right hand pane right click on **Named Pipes**, select **Enable**, and click **OK** at the confirmation message.

4. In the right hand pane, right click on **TCP/IP**, select **Enable**, and click **OK** at the confirmation message.

5. In the left hand pane, click on **SQL Server Services**, then right click on **SQL Server (MSSQLSERVER)** and select **Restart** to restart the SQL Server process.

6. Close the SQL Server Configuration Manager window.

3.2.3 Configure Windows Firewall for SQL Server

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

1. In **Server Manager**, click **Tools**, select **Windows Firewall with Advanced Security** and click **Inbound Rules**. A list of firewall rules is displayed.

2. In the **Actions** pane, click **New Rule**. The New Inbound Rule Wizard is displayed.

3. Select **Port** as the rule type and click **Next**.

4. Select **TCP** as the protocol and enter **1433** as the specific local port. **Click** Next. The Action options are displayed.

5. Choose **Allow the connection**. Click **Next**. The Profile options are displayed.

6. Select the profile options that are appropriate to your deployment and click **Next**.

7. Enter a name for the rule and click **Finish** to create the rule. The new rule appears in the list of inbound rules as an enabled rule.

8. Close the Server Manager window.

3.2.4 SQL Server Backup Guidelines

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

3.3 User Accounts

3.3.1 Unified CCMP Service Accounts

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

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

SQL Agent User

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

> **Note**
>
> For single-sided installations containing a single all-in-one server, you can choose to allow Unified CCMP to create this account automatically as a local account. But if you choose this option, then want to add additional servers to your deployment later, you will need to reinstall the system.

To create the required account:

1. Using Active Directory, create the domain account **sql_agent_user** (or a name of your choice) with the following attributes:

    *   Password never expires
    *   User cannot change password.

3.4   Optional Security Configuration

3.4.1   Disable Anonymous Sessions

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

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

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

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

then enable the setting

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

Alternatively, you can update the registry directly as follows:

1. In the **Run** command dialog box, enter **regedit**.

2. In the left hand pane, select the **HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Control\Lsa** node.

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

4. Close the registry editor.

3.4.2   Disable Cached Logins

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

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

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

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

then set the following setting to **0**

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

Alternatively, you can update the registry directly as follows:

1. In the **Run** command dialog box, enter **regedit**.

2. In the left hand pane, select the **HKEY_LOCAL_ MACHINE\Software\Microsoft\Windows Nt\CurrentVersion\Winlogon** node.

3. In the right hand pane, if the REG_SZ value **CachedLogonsCount** is present, set it to 0, otherwise, create it and set it to 0. Click **OK**.

4. Close the registry editor.

3.4.3   Disable DCOM

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

This security setting applies to all Unified CCMP servers.

1. Launch **Component Services** (from the **Administrative Tools** group).

2. Expand **Component Services**, and then **Computers**. Right-click on **My Computer** and select **Properties**.

3. Select the **Default Properties** tab and clear **Enable Distributed COM on this computer**. Click **OK**, then **Yes** when asked to confirm that you want to update the DCOM Settings.

4. Close the Component Services dialog box, then reboot the server.

3.4.4 Enable Mandatory SMB Signing for all Unified CCMP Servers

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

This security setting applies to all Unified CCMP servers.

1. In **Server Manager**, click **Tools** and select **Local Security Policy**. Navigate to **Local Policies > Security Options**.

2. In the right hand pane, click on **Microsoft network client: Digitally sign communications (always)**. Select **Enabled** and click **OK**.

3. In the right hand pane, click on **Microsoft network server: Digitally sign communications (always)**. Select **Enabled** and click **OK**.

4. Close the Local Security Policy dialog box.

5. On every client that needs to communicate with the Unified CCMP servers (including all clients running the Web UI), ensure that the following security options are set in the local security policy (launch **Server Manager**, click **Tools** select **Local Security Policy** and navigate to **Local Policies > Security Options**):

    *   **Microsoft network client: Digitally sign communications (always)**: ensure this is **Disabled** (the default value), unless other systems specifically require it to be enabled .

    *   **Microsoft network client: Digitally sign communications (if server agrees)**: ensure this is **Enabled** (this is the default value).

3.4.5 Disable SSL V2

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

On each App/Web Server:

1. In the **Run** command dialog box, enter **regedit**.

2. In the left hand pane, select the **HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\S CHANNEL\Protocols\SSL 2.0** node.

3. If the registry key **Server** does not exist, right-click the **SSL 2.0** node, select **New > Key**, and create it.

4. Under the registry key **Server**, create a **DWORD** value named **Enabled** and set the value data to **00000000**.

5. Close the registry editor and reboot the server.

3.4.6 Disable Remote Access to Unified CCMP Servers

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

4   Unified CCMP Installation

4.1   Before You Start

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

4.1.1   Installing Dual-Sided Systems

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

4.1.2   Recording Your Settings

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

System Setting	Value
Database Catalog Name	
sql_agent_user Password	
Cryptographic Passphrase	
Administrator Password	
Java.RMI.Hostname	

System Setting	Value
Unified CCE	
Application Name	
Application Key	
RMI Registry Port	
LocalPort	

4.2   The Unified CCMP Installer

4.2.1   About the Unified CCMP Installer

4.2.1.1   Starting the Installer

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

- If auto-run is enabled, a window opens automatically showing a list of Unified CCMP components that can be installed.

- If auto-run is disabled and you do not see the Installation Components screen, double-click **autorun.bat** to launch the Unified CCMP installer manually.

- If UAC has not been disabled, launch the installation manually by right-clicking **autorun.bat** and selecting **Run as administrator** option.

Note

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

4.2.1.2   Installation Prerequisites

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

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

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

4.2.2   Install the Database Installer

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

On the Side A Database Server:

1.   Insert the Unified CCMP DVD and start the Unified CCMP Installer (for more information about the Unified CCMP Installer, see section 4.2.1 "About the Unified CCMP Installer").

2.   Select **Database Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.

3.   When all checks have passed, click **Install**. At this point, the Informix client is installed first if necessary. If you see the Informix client installation screen, click **Install**.

4.   When the Informix client has been installed, the installation of the Database Installer starts, and the **Setup** window displays.

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

6.   In the **License Agreement** window:

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

7.   In the **Cryptography Configuration** window:

   •   **Passphrase.** Create a cryptographic passphrase of between 6 and 35 characters. This passphrase is used for encrypting and decrypting system passwords and must be the same for all servers in the Unified CCMP installation.

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

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

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

8. In the **Configure Database** window:

    * **Database Name**. Enter the name of the database catalog for Unified CCMP. By default this is **Portal**.

    * **Connect Using**. Select the login credentials you want to use:

        * **Windows Authentication Credentials of Application**. This is the recommended option.

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

    * Click **Next**.

9. In the **Destination Folder** window, if you want to change the location where the database components are stored, click **Change** and select the new location. It is not necessary to install all Unified CCMP components in the same location.

10. Click **Install** to install the Database Installer. During this process, the J2SE prerequisite will be automatically installed if it is not already present. If this happens, follow the screen prompts to complete the J2SE installation. If you see a Security Alert dialog box during the installation, saying 'Revocation Information for the security certificate for this site is not available', click **Yes** to continue.

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

12. Click **Finish**.

4.2.3   Install the Portal Database

> **Note**
>
> The installation of the Portal Database will fail unless the SQL Server installation has been configured to use US English. If this is not the case, instructions for changing the installation language are given in section 12.2 "Changing the SQL Server Installation Language to US English".

To install the portal database:

1. If you selected the Launch Database Management Utility check box after installing the Database Installer, the database setup wizard will start automatically. Otherwise launch the Unified CCMP **Database Installer**.

2. Click **Next** to begin the installation.

3. In the **Select an Action to Perform** window, choose **Install a new database** You can maintain this database at a later date by running the installer again and selecting the appropriate option.

4. In the **SQL Server Connection Details** window:

   - **Server Name.** Enter the name of the machine that is to be the Database Server. This should normally be left as the default (**localhost**).

   - **Database Name.** Enter or select the name of the database catalog that will be used for Unified CCMP. It is recommended that you use the default name of **Portal**. This should match the database catalog name specified when you installed the database installer. If not, you will see a warning message.

   - **Connect Using.** Select the login credentials you want to use:

     - **The Windows account information I use to logon to my computer.** This is the recommended option.

     - **The SQL Server login information assigned by the system administrator.** Only select this option if you are using a database catalog on a different domain. For this option you must enter your SQL Server Login Name and Password in the fields provided.

   - Click **Test Connection.** This makes sure the connection to the SQL Server is established. If the connection can be established, you will see the message 'Connection succeeded but database does not exist'.

   - Click **Next**.

5.   In the **Setup Replication** window, if this database installation is not Side B of a replicated system, just click **Next**. If this database installation is Side B of a replicated system, select **Replicated Configuration** and set up the replication folder share as follows:

  •   **Share Name** The name of the share for the ReplData folder. By default this is **ReplData**.

  •   **Folder Path** The path of the ReplData folder. This is configured in SQL Server, and is by default **C:\Program Files\Microsoft SQL Server\MSSQL\repldata.**

  •   Click **Next**.

6.   In the **Configure the Location of Data Files** window:

  a.   Click **Select All**.

  b.   Select **Set Initial Size to Max Size**.

  c.   Click **Update**.

  d.   Click **Select None**.

  e.   Select each file in the File Group list in turn. For each:

    i.   Refer to the table of file group names and sizes below and change the **Max Size** for the file group to the value shown for that file in the table.

    ii.   Click **Update**.

    iii. Clear the selection.

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

  f.   Click **Next**.

File Group Name	Size
adminfilegroup	3310
adminindexfilegroup	830
dimfilegroup	11580
dimindexfilegroup	3310
factfilegroup	4100
factindexfilegroup	8210
fctauditfilegroup	1650

File Group Name	Size
fctauditindexfilegroup	1852
fctcmsfilegroup	3310
fctcmsindexfilegroup	500
fctetlauditfilegroup	1650
fctetlauditindexfilegroup	250
fctfilegroup	1650
fcticmfilegroup	9920
fcticmindexfilegroup	1490
fctindexfilegroup	250
fctinfilegroup	1650
fctinindexfilegroup	250
fctivrfilegroup	8270
fctivrindexfilegroup	1240
fctmmfilegroup	3310
fctmmindexfilegroup	500
fctwfmfilegroup	1650
fctwfmindexfilegroup	250
logfilegroup	17575
primaryfilegroup	6620
secfilegroup	3310
secindexfilegroup	830
stagingfilegroup	8270
stagingindexfilegroup	3310
sumcmsfilegroup	6620
sumcmsindexfilegroup	990
sumfilegroup	290

File Group Name	Size
sumicmfilegroup	6620
sumicmindexfilegroup	990
Sumindexfilegroup	290
suminfilegroup	6620
suminindexfilegroup	990
sumivrfilegroup	6620
sumivrindexfilegroup	990
summmfilegroup	6620
summmindexfilegroup	990

7.   The **Configure SQL Server Agent Service Identity** window sets up a user account that is used by SQL Server for replication:

- **Account Type** The type of user account that will be used. For a distributed installation, this must be **Domain**.

- **User Name** The name of the SQL agent user account. This defaults to **sql_agent_user**. If you have not already created this account, set it up now as described in section 3.3 "User Accounts". If you used a different name when setting up the account, enter that name instead. If you have specified a domain user, you will need to prefix the user name with the domain name, followed by a backslash. For example if the SQL agent user belongs to the **UCCMPDOM** domain then enter **UCCMPDOM\sql_agent_user**.

- **Automatically create the user account if missing** For a single-sided system that contains a single all-in-one server, you can optionally select this check box and create the required user automatically. But if you select this option and need to add a additional servers in future, you will need to reinstall the system.

- **Password** If you are using an existing SQL agent user account, enter the password for that account. Otherwise, if you have a single-sided system and are creating the account automatically, create a password for the new user, conforming to the complexity requirements for your system.

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

- Click **Next**.

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

> **Note**
>
> If the installation reports an error saying that the SQL Server language must be US English, you will need to fix this before you can install the Portal Database. For instructions, see section 12.2 "Changing the SQL Server Installation Language to US English". Then repeat the installation of the Portal Database.

9. Click **Close** to close the installer.

4.2.4   Install the App/Web Server

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

On the Side A App/Web Server:

1. Insert the Unified CCMP DVD and start the Unified CCMP Installer (for more information about the Unified CCMP Installer, see section 4.2.1 "About the Unified CCMP Installer").

2. Select **App/Web Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.

3. When all checks have passed, click **Install** to begin the App/Web Server installation. The **Management Portal: Application Server Components** window displays.

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

5. If the Management Portal: Application Server Components Dialog is displayed, click **Install** to install the additional required components.

6. If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.5 Framework is complete, restart the server to continue the installation of the App/Web Server.

7. In the **License Agreement** window:

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

8. In the **Cryptography Configuration** window:

   • **Passphrase**. Enter the cryptographic passphrase you used for the installation of the Database Server component.

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

   • Click **Next** to continue.

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

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

10. In the **Configure Database** window:

    • **SQL Server Name**. Enter the host name or IP Address of the server hosting the Unified CCMP database. The default name of **localhost** is only valid if you are installing this component on the Database Server. Otherwise, specify the name of the Database Server. For a dual-sided deployment enter the name of the Side A Database server when installing the Side A components and enter the name of the Side B Database Server when installing the Side B components.

    • **Catalog Name**. Enter or select the database catalog name you specified when installing the Database Server component. If you used the default value, this will be **Portal**.

    • **Connect Using**. Select the login credentials you want to use:

        • **Windows authentication.** This is the recommended option.

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

    • Click **Next** to continue.

11. Click **Install**.

12. When the installation has completed, click **Finish**. When installation is complete, the machine will restart.

4.2.5   Install the Second Side (Replicated Systems Only)

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

4.3   Support Tools

4.3.1   About the Support Tools

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

4.3.2   Install the Diagnostic Framework

1. To install the Diagnostic Framework component, start the Unified CCMP Installer, click **Support Tools** and select **Diagnostic Framework**. The **Management Portal: Diagnostic Framework InstallShield Wizard** window displays.

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

3. In the **License Agreement** window:

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

    *   Click **Next**.

4. In the **Select Certificate** window, select the type of certificate installed with the Diagnostic Framework.

    *   **Self Signed**. A new certificate will be generated by the installer. This type of certificate should be used only for lab or test deployments.

    *   **Trusted Certificate**. An existing certificate issued by a valid certificate server will be associated at a later date. This option should be used for production deployments.

    *   Click **Next**.

5. In the **wsmadmin Password Information** window, enter the password for the **wsmadmin** user that will be created to access the Unified System CLI tool. Enter your chosen password again to confirm it. Click **Next**.

6. Click **Install**.

7. When the installation is completed, click **Finish**.

The installation of the Diagnostic Framework component is now complete.

5   Unified CCMP Configuration

5.1   About Unified CCMP Configuration

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

This section describes the following steps:

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

5.2   Configure Unified CCE Admin Workstations

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

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

1.   Login to the AW as a user with local administrative privileges.

2.   Launch SQL Server Management Studio. Connect to the server.

3.   Open up the **Security** folder, and right-click **Logins**.

4. Select **New Login** from the drop-down list. The Login – New window displays.

5. Add SQL logins for the Network Service accounts of each server hosting Unified CCMP (Database Servers and App/Web Servers), by filling in the fields as follows:

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

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

6. Click **OK**.

5.3 Configure Unified CCE Provisioning

5.3.1 About Provisioning Configuration

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

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

- Unified CCMP Resource Management uses Cisco ConAPI for the Provisioning connections: this interface requires that all connections are made to a Primary Distributor AW. If the AW is dual-sided, both sides must be Primary Distributors.

- Multiple Unified CCE instances can be supported, but each requires a distinct primary Distributor AW to connect to:
    - ConAPI only supports connection to one Application Instance on each physical server. You must therefore have a separate physical AW distributor for each instance.
    - Parent/Child AW configurations are supported as multiple instances in Unified CCMP.

Note

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

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

5.3.2 Set Up ConAPI

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

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

Note

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

2. Under **Tools > List Tool**s you will find the **Application Instance List**. Double-click this to open it.

3. Click **Retrieve** to display the list of configured application instances. You can use an application instance from this list for Unified CCMP or create a new one. To create a new application instance, click **Add**, and enter the following details:

    ● **Name** A unique name to be used for the application instance.

    ● **Application Key** A password to be used by Unified CCMP to connect. This may be between 1 and 32 characters.

    ● **Confirm Application Key** Ensure that no typographical errors were made while choosing the application key.

    ● **Application Type** Select **Cisco Voice**.

    ● **Permission Level** Give the application full read/write permissions.

4. Record these details for use during the configuration of the cluster.

5. Click **Save** and then click Close.

5.3.3 Set Up the CMS Server

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

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

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

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

1.   On the Unified CCE being configured, launch **CMS Control**. This opens the CMS control console.

2.   Click **Add** on the right hand side of the window to launch the **Application connection details** window and fill in the fields as follows:

   • **Administration & Data Server Link**. The name of the Unified CCMP Database Server, in capital letters, with **Server** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBServer**.

   • **Administration & Data Server RMI registry port.** The port on the Unified CCE AW for the Unified CCMP Provisioning service to connect to. This will usually be 2099, but if the Unified CCMP Provisioning service is connecting to multiple Unified CCE instances, each Unified CCE instance should use a different port.

   • **Application link**. The name of the Unified CCMP Database Server, in capital letters, with **Client** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBClient**.

   • **Application RMI registry port**. The port on the Unified CCMP Database Server for the Unified CCE AW to connect to. For convenience, this should be the same as for the ICM Distributor AW RMI registry port specified above. Each Unified CCE AW must connect to a different port on the Database Server. You should record this information for future use.

   • **Application host name**. The name of the Unified CCMP Database Server, in capital letters, for example, **PRODUCTDB**.

3.   Click **OK**, and **OK** again to cycle the CMSJServer, save your changes and close the CMS control console.

5.4 Configure the Unified CCMP Cluster

5.4.1 About Cluster Configuration

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

* configure the servers in the Unified CCMP cluster (the Unified CCMP servers, Unified CCEs and Unified Communications Managers)

* set up the equipment mappings between remote tenants and Unified CCMP resources.

Follow the instructions below to configure your system when you first install it. For more information about using the ICE tools to modify your system configuration at a later date, see the *Integrated Configuration Environment (ICE) for Cisco Unified Contact Center Management Portal*.

5.4.2 Start ICE Cluster Configuration

To start ICE, on the Side A Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

   * **Server Name**. Enter the name of the primary database server.

   * **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

   * **Authentication**. Select Windows Authentication.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. In the ICE Cluster Configuration tool, select the **Setup** tab in the left hand pane. This displays a series of wizards to set up the servers.

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

5.4.3 Set Up Unified CCMP Servers

5.4.4 About the Setup Unified CCMP Servers Wizard

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

5.4.5   Setting Up the Unified CCMP Servers

Note

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

To set up the Unified CCMP servers:

1.   In the ICE Cluster Configuration tool, select the **Setup** tab and click **Setup UCCMP Servers** to start the wizard. Click **Next** to go through each window in turn.

2.   On the **Select Deployment Type** page, select your chosen deployment type.

3.   On the **Configure Redundancy** page, select whether you would like to configure a single-sided or a dual-sided system. Click **Next**.

4.   If you are performing a two tier deployment then you will be asked to enter the number of web servers for each side. Enter the number of app/web servers on each side of your deployment. Dual-sided configurations must have an equal number of app/web servers on each side. Click **Next**.

5.   On the **Configure Servers** pages, enter the server names for each of the Unified CCMP servers. The number of pages and servers to specify will depend on the deployment options you chose above.

6.   On each page, enter the following, then click **Next**:

   •   **Primary Server**

      •   **Server Name**. This is the non-domain qualified machine name.

      •   **Server Address**. This defaults to Server Name. This can be changed to an IP Address or a domain qualified name of the server.

   •   **Secondary Server**:

      •   If you chose a dual-sided setup, provide the corresponding details for the Side B server.

7.   Click **Next** and enter the relevant server information for each Unified CCMP server until you reach one of the following pages: **Primary Database Administrator Login**, **Secondary Database Administrator Login** or **Configure Relational Database Connection**.

Note

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

8. If the **Primary Database Administrator Login** page is shown, provide details of a SQL Server user account on the primary database server that has sufficient permissions to create new SQL Server users and grant permissions to them. This account is used to set up the users and permissions required by Unified CCMP to connect the Unified CCMP services to the portal database. This account is only used during system setup.

   • **Authentication**. Select the authentication mode for this user.

      • **Windows Authentication**. Select this option to use the currently logged in Windows domain user.

      • **SQL Authentication**. Select this option to use a specific SQL Server user. Either accept the default **sa** user (created when the Unified CCMP database was installed, and which does have sufficient permissions) or enter another SQL Server user, then specify the password.

   • Click **Next**.

9. If you have specified a dual-sided installation, and the **Secondary Database Administrator Login** page is shown, follow the instructions in step 8. to provide details of a database user account with sufficient privileges on the secondary database server.

10. On the **Configure Relational Database Connection** page, enter the connection details to be used by each Unified CCMP server to connect to the Unified CCMP portal database:

   • **Catalog**. This is the name of the Unified CCMP database. The default is **Portal**.

   • **Authentication**. Select the authentication mode to use to connect to the Unified CCMP database.

      • **Windows Authentication**. The recommended authentication mode. If this mode is selected, each Unified CCMP service will connect to the portal database using the Windows account under which the service is running (by default, all Unified CCMP services run under the Network Service account).

- **SQL Authentication**. Only select this option if you are using a Database Server on a different domain. For this option you must enter the SQL Server username and password in the fields provided.
- Click **Next**. If you selected SQL Authentication and the specified account does not yet exist, you will be prompted to create it.

11. The **Deployment Summary** page summarizes the choices you have made.

12. Check the deployment details, and if you are satisfied, click **Next**.

13. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.

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

5.4.6   Configure Cisco Unified CCE Servers

5.4.6.1   About the Configure Cisco Unified CCE Servers Wizard

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

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

5.4.6.2   About Unified CCE Deployment Models

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

- Administration Server and Real-time Data Server (AW)

5.4.6.3   About Unified CCMP Connection Requirements

Depending on the deployment model, Unified CCMP may require a connection to:

- Unified CCE real-time AWDB for data import
- Unified CCE AW for Unified CCMP Provisioning Server requests.

5.4.6.4   **Configuring Cisco Unified CCE Servers**

> **Note**
>
> This wizard configures the Unified CCE servers using an SQL Connection. You will need to know the connection credentials to complete the configuration.
>
> If you require resource management (provisioning), you will also need to know the login details for a user with appropriate access to the Unified CCE used for provisioning. On the domain controller, this user must be in the domain security group **<Server>_<UCCEInstance>_Config**, where *<Server>* is the name of the server running Unified CCE and *<UCCEInstance>* is the name of the Unified CCE Instance on this server.

To configure the Cisco Unified CCE servers:

1.   In the ICE Cluster Configuration tool, select the **Setup** tab and click **Configure Cisco Unified CCE Servers** to start the wizard. Click **Next** to go through each page in turn.

2.   On the **Select Task** page, select the action. The options are:

   •   Add a new instance

   •   Modify an existing instance

   •   Remove an existing instance.

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

3.   On the **Specify Resource Name** page, specify the name for the instance being configured. You can use the default name or choose another name.

4.   On the **Select Required Components** page, select all the required components in the deployment.

   •   **Admin Workstation**. Select this component for all configurations.

   •   **ConAPI Server (Provisioning)**. Select this component if you require resource management.

5.   On the **Configure Redundancy** page, select whether you want to configure a single-sided or a dual-sided setup.

6.   On the **Configure AW Server** page, enter the following:

   •   **Primary Server**:

- **Server Name**. This is the non-domain qualified machine name where the Admin Workstation and ConAPI components are deployed.

- **Server Address**. This defaults to Server Name. This may be changed to an IP Address or a domain qualified name of the server.

- **Secondary Server**:

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

7. On the **Configure Connection Details** page, enter the authentication details to connect to the Admin Workstation database.

    - **Windows Authentication.** This is the default recommended authentication mode.

    - **SQL Authentication**. If this mode is chosen then specify the SQL Server user name and the corresponding password to connect to the databases.

8. On the **Select Unified CCE Instance** page, select the AW instance to be used in the deployment. Click **Next**.

9. On the **Configure Primary Unified Config Web Service** page, (only shown if the Unified CCE instance is running Unified CCE version 9.0 or later), enter the following details

    - **URL**. This is the auto-generated URL of the primary unified config web service on the Unified CCE

    - **User Name**. This is a username with appropriate access to the Unified CCE that the web service is running on. This user must be in the domain security group **<Server>_<UCCE-Instance>_Config**, where *<Server>* is the name of the server running Unified CCE and *<UCCE-Instance>* is the name of the Unified CE Instance on this server. For Unified CCE version 9.0(1) or 9.0(2), enter the username as **<domain>\<user>** and for Unified CCE version 9.0(3) or later, enter the username as **<user>@<domain>**, where <user> is the Unified CCE username, and <domain> is the name of the domain.

    - **Password**. This is the password for the user.

10. On the **Configure Primary ConAPI RMI Ports** page, (only shown if you selected the ConAPI Server (Provisioning) option above) enter the following ConAPI details:

- **Local Registry Port.** This is the port on the Unified CCE for the Unified CCMP Provisioning service to connect to. This will usually be 2099.

- **Remote Registry Port.** This is the port on the Unified CCMP Database Server for the Unified CCE to connect to. This will usually be 2099.

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

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

11. On the **Configure ConAPI Application Instance** page (only shown if you selected the ConAPI Server (Provisioning) option above), enter the following details:

    - **Application Name.** The name of the application to be used for provisioning Unified CCE from Unified CCMP. Specify the name of the application you configured in section 5.3.2 "Set Up ConAPI" Credentials.

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

12. On the **Multi Media Support** page, select **Yes** if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance to provide support for non-voice interactions. The default is No.

13. On the **Purge On Delete** page, select **Yes** if you want to purge items from Unified CCE automatically when they are deleted from Unified CCMP. The default is Yes.

14. On the **Supervisor Active Directory Integration** page, select **Yes** if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors. The default is No. If you select Yes then you will be prompted to provide Active Directory information so that Windows user accounts can be listed.

15. On the **Configure Linked Unified CM Servers** page, select the Unified Communications Manager servers that the Unified CCE being configured is capable of routing calls to.

Note

The Configure Linked Unified Communications Manager Servers page only appears if at least one Unified Communications Manager server has been configured. You can also link the Unified Communications Manager servers to Unified CCE from the Unified Communications Manager Configuration Wizard, or modify the Unified CCE configuration later to link to the Unified Communications Manager servers.

16. The **Summary** page summarizes the details of the Unified CCE being configured and the settings you have chosen.

17. Check the details, and if you are satisfied, click **Next**.

18. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.

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

5.4.7 Configure Cisco Unified Communications Manager Servers

5.4.7.1 About the Configure Cisco Unified Communications Manager Servers Wizard

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

- add a new Cisco Unified Communications Manager instance to the deployment

- update an existing Cisco Unified Communications Manager instance in the deployment

- remove an existing Cisco Unified Communications Manager instance from the deployment.

5.4.7.2 Configuring Cisco Unified Communications Manager Servers

To configure the Cisco Unified Communications Manager servers:

1. In the ICE Cluster Configuration tool, select the **Setup** tab and click **Configure Cisco Unified Communications Manager Servers** to start the wizard. Click **Next** to go through each page in turn.

2. On the **Select Task** page, select the action. The options are:
   - Add a new instance

- Modify an existing instance
- Remove an existing instance

Note

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

3. On the **Specify Resource Name** page, specify a name for the instance being configured. You can use the default name or choose another name.

4. On the **Configure Unified CM Servers** page, enter the following:

- **Primary Server**

  - **Sever Name**. This is the non-domain qualified machine name where the Cisco Unified Communications Manager components are deployed.

  - **Server Address**. This defaults to Server Name. This can be changed to an IP Address or a domain qualified name of the server.

Note

When configuring a Unified Communications Manager Cluster ensure that only the publisher of the cluster is configured.

- **Secondary Server**: This option is always disabled.

5. On the **Select Version** page, select the version of Unified Communications Manager being configured from the drop-down list.

6. On the **Connection Details** page, enter the following details:

- **URL**. This is used to access the Unified Communications Manager AXL interface. The default is the default URL for the Unified Communications Manager version that has been selected. It is recommended that you use the default URL.

- **User Name**. This is the name of the Unified Communications Manager Administrator user. This is the user name that the Unified CCMP components use when connecting to the Unified Communications Manager AXL web service.

- **Password**. This is the Unified Communications Manager Administrator user's password.

7. On the **Configure Linked Unified CCE Servers** page, select the configured Cisco Unified CCE servers that can route calls to the Unified Communications Manager being configured.

> **Note**
> The Configure Linked Unified CCE Servers page only appears if at least one Unified CCE server has been configured. You can also link the Unified Communications Manager server to Unified CCEs from the Cisco Unified CCE Configuration Wizard, or modify the Unified Communications Manager configuration later to link to the Unified CCE servers.

8. The **Summary** page summarizes the details of the Unified Communications Manager being configured and the settings you have chosen.

9. Check the details, and if you are satisfied, click **Next**.

10. A confirmation message is displayed to indicate that the wizard has completed successfully. Click Exit to close the wizard.

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

5.4.8   Configure Cisco Unified CVP Servers

5.4.8.1   About the Configure Cisco Unified CVP Servers Wizard

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

This wizard guides you through the steps to:

- add a new Cisco Unified CVP cluster instance to the deployment

- update an existing Cisco Unified CVP cluster instance in the deployment

- remove an existing Cisco Unified CVP cluster instance from the deployment.

5.4.8.2   Configuring Cisco Unified CVP Servers

To configure a Cisco Unified CVP server cluster:

1. In the ICE Cluster Configuration tool, select the **Setup** tab and click **Configure Cisco Unified CVP Servers** to start the wizard. Click **Next** to go through each page in turn.

2. On the **Select Task** page, select the action. The options are:
   - Add a new instance
   - Modify an existing instance
   - Remove an existing instance.

   The Modify and Remove options are only enabled when at least one Cisco Unified CVP cluster instance has already been configured.

3.   On the **Specify Unified CVP Operations Console Resource Name** page, specify a name for the Unified CVP operations console.

4.   On the **Select Version** page, specify the version of Unified CVP that is running on the CVP cluster you are configuring.

5.   On the **Configure Unified CVP Operations Console** page, enter the following:

   * **Primary Server**:

      * **Sever Name**. This is the non-domain qualified machine name where the Cisco Unified CVP Operations Console is deployed.

      * **Server Address**. This defaults to Server Name. You can change this to an IP Address or a domain qualified name of the server.

   * **Secondary Server**: This option is always disabled.

6.   On the **Configure Primary Unified Config Web Service** page (only shown when the selected Unified CVP version is 10.0 or later), enter the following details:

   * **URL**. This is the auto-generated URL of the primary unified config web service on the Unified CVP cluster.

      * **User Name**. This is a username with appropriate access to the Unified CVP that the web service is running on.

      * **Password**. This is the password for the user.

7.   On the **Select Number of Call Servers** page, specify the number of CVP call servers in the CVP cluster.

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

8.   If you specified at least one call server:

   a.   On the **Specify Unified CVP Call Server 1 Resource Name** page, enter a name for the call server.

   b.   On the **Configure Unified CVP Call Server 1** page, enter the following:

   * **Primary Server**:

      * **Sever Name**. This is the non-domain qualified machine name of the Cisco Unified CVP call server.

      * **Server Address**. This defaults to Server Name. You can change this to an IP Address or a domain qualified name of the server.

- **Secondary Server**: This option is always disabled.

9. If you specified more than one call server, repeat step 8. to provide the details for the each of the remaining call servers.

10. The **Summary** page summarizes the details of the Unified CVP cluster being configured and the settings you have chosen.

11. Check the details, and if you are satisfied, click **Next**.

12. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.

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

5.4.9 Create and Map Tenants

5.4.9.1 About Creating and Mapping Tenants

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

- create the Unified CCMP folder structure for your deployment
- specify the rules for importing resources into your Unified CCMP folder structure from the contact center equipment (for example, Unified CCE, Unified Communications Manager).

5.4.9.2 Creating Tenants and Folders

To create a Unified CCMP tenant:

1. In the ICE Cluster Configuration tool, select the **Equipment Mapping** tab. In the center pane, right click on the root node and select Add Tenant.

2. In the **Name** field enter the name of the tenant, and optionally, in the **Description** field, enter a description.

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

To create a Unified CCMP folder:

1. In the ICE Cluster Configuration tool, select the **Equipment Mapping** tab. In the center pane, right click on the folder tree at the location where you want to add the folder and select Add Folder.

2. In the **Name** field enter the name of the folder, and optionally, in the **Description** field, enter a description.

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

5.4.9.3 Creating an Equipment Mapping

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

1. In the ICE Cluster Configuration tool, select the **Equipment Mapping** tab. In the folder tree, select the tenant or folder where you want to place the resources you import from the contact center equipment.

2. In the adjoining pane select the check box next to each item of contact center equipment you want to associate with the selected folder or tenant.

3. Highlight each selected item in turn, and, in the right hand pane, select one of the following:

    •   **Default Import Location**. All resources from the highlighted contact center equipment will be imported into the selected folder or tenant in Unified CCMP. You may see a warning if you select this option. If the selection was intentional, you can ignore the warning.

    •   **Customer Resource Mapping**. Allows more control over the import process. You can specify the items on the highlighted contact center equipment to be placed in the selected folder or tenant in Unified CCMP. If you select this option you can:

        •   Click ✚ to add a new customer resource mapping that defines the resource types and the specific resources of that type to be mapped to the selected import location. Select the resource type from the **Type** drop-down list (one of Peripheral, Routing Client, Media Routing Domain and Remote Tenant) then select the specific item of that type that you want to map from the **Resource** drop-down list. Click **OK**. Repeat to map other customer resources on this item of contact center equipment to the specified import location.

        •   Click ✖ to delete an existing customer resource mapping.

Note

If you want to use the customer resource mapping option, you will not be able to configure this until you have imported the customer resources you want to use to define the mappings.

In this case, for the first import, **do not** select the Default Import Location option, as once you have selected this, the items from the remote equipment will be imported to that location and cannot be re-imported. Instead, for the first import, **do not specify any import location**, so everything is imported into the **/Unallocated** folder. Once the customer resources have been imported, you can specify the customer resource mapping you require, and the items in the **/Unallocated** folder will be moved to the required locations.

Note

If Customer Resource Mapping is selected then any resources on the contact center equipment that are not associated with the selected mapping will be placed in the source equipment subfolder under the Unallocated folder.

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

5.5   Replication

5.5.1   About Replication

5.5.1.1   About the Replication Manager

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

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

When your system is first installed you should:

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

For more information about using the ICE Replication Manager to manage replication at a later date, see the *Integrated Configuration Environment (ICE) for Cisco Unified Contact Center Management Portal*.

5.5.1.2 About The Snapshot Process

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

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

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

5.5.1.3 About Replication Publications

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

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

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

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

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

5.5.2   Configure Replication

> **Note**
>
> The user running Replication Manager must have administrator permissions in both Windows and SQL Server, for both the publisher and subscriber Database Servers.
>
> Before configuring replication you should have already configured Unified CCMP in dual-sided mode using the Cluster Configuration tool as described in section 5.4 "Configure the Unified CCMP Cluster".

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

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

    - **Server Name**. Enter the name of the primary database server.

    - **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

    - **Authentication**. Select Windows Authentication.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. From the Tool drop-down list, select **Replication Manager**. The Replication Manager opens in the Setup tab. The Setup tab has the following sections:

    - **Unified CCMP Database Server Properties** contains the publisher and subscriber Unified CCMP database details.

    - **Distributor Properties** contains the SQL Server Replication distributor properties.

    The default values shown in the Setup tab are derived from the values initially configured in the Cluster Configuration tool and will be suitable in most cases.

4. If required, modify the Unified CCMP Database Server Properties.

    - **Server Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.

    - **Catalog Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration. It may be changed, but if so, a valid database with the new name must already exist on the corresponding server.

5. If required, modify the distributor properties.

- **Server Name**. The name of the subscriber server hosting the Unified CCMP database. This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.

- **Catalog Name**. The name to be assigned to the distribution database. The recommended value is **distribution_portal**.

- **Data Folder**. The folder path on the distributor server where the data file for the distribution database will be created.

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

- **Log Folder**. The folder path on the distributor server where the transaction log file for the distribution database will be created.

- **Distribution Share**. The distribution share folder where replication snapshot files will be generated.

- **Override Distributor Admin Password**. Select to override the auto-generated replication password which will be used to establish connectivity. The auto-generated password is 14 characters long, and will contain alpha-numeric characters (both upper and lower case) and a special character. If this does not meet the complexity requirements of the server then select this option and specify a password of your choice.

6.   When you have set the required replication properties, click **Configure** to configure replication.

7.   You may be prompted to save pending changes to the database before continuing. If so, click **Yes** to save pending changes and continue.

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

5.5.3   Monitor the Replication Snapshot

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

To monitor the progress of the replication snapshot:

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

    - **Publications** (top left) lists the publisher servers and the publications on each publisher that need to be shared with the subscribers.

    - **Subscriptions and Agents** (top right) shows the subscriptions to a publication and the replication agents associated with a publication. This pane has two tabs, Subscriptions and Agents.

    - **Subscriptions** shows the subscriptions to the selected publication. You can right-click on a subscription to start or stop the subscription.

    - **Agents** shows the replication agents associated with the selected publication. You can right-click on a replication agent to start or stop the agent.

    - **Sessions** (bottom left) shows all sessions for the selected publication and replication agent in the last 24 hours.

    - **Actions** (bottom right) shows the activity for the selected session.

2. In the top left hand pane, select the first Unified CCMP database publication from the list of publications. If you have used the default database name, this will start with **[Portal]**.

3. Wait for the replication snapshot for this publication to complete.

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

    "Delivered snapshot from . . . "

    "No replicated transactions are available".

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

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

4. Repeat the two steps above for each of the remaining Unified CCMP database publications.

5. When replication is complete for all portal database publications, close the ICE tool.

The subscriber database can now be used to service requests. For more information about the Replication Manager see the *Integrated Configuration Environment (ICE) for Cisco Unified Contact Center Management Portal*.

6 Post-Installation Steps

6.1 About Post-Installation Steps

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

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

6.2 Configure SSL

6.2.1 About Configuring SSL for Unified CCMP

Follow the instructions below to configure SSL for the Unified CCMP web application.

> **Note**
>
> These steps are mandatory and some features of the Unified CCMP web application will not work properly unless you do this.
>
> These steps are also required if you are upgrading Unified CCMP, even if you have already configured SSL for a previous version.

To configure SSL for Unified CCMP you need to:

- obtain a digital certificate if you do not already have a suitable one (see section 6.2.2 "Obtain a Digital Certificate")

- export the certificate in PFX format (see section 6.2.3 "Export the Certificate in PFX Format")

- configure SSL for the Unified CCMP web application (see section 6.2.4 "Configure SSL for the Web Application").

6.2.2   Obtain a Digital Certificate

If required, a digital certificate may be obtained in either of the following ways:

- purchased from an external certificate authority, for public use

- generated internally, for secure use within the issuing organization.

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

1.   Open **Internet Information Services (IIS) Manager** and select the web server in the folder hierarchy.

2.   Select the **Features View** tab, and in the **IIS** group, click on **Server Certificates**.

3.   Create a digital certificate in one of the following ways:

> **Note**
>
> The Common Name is the application domain name. Take care to enter it exactly as specified here. The certificate will not work otherwise. The Common Name is derived as follows:
>
> - For deployments with a registered address (including load-balanced deployments) enter the registered address, starting from **www**. For example, if your registered address is **https://www.Unified CCMP.com**, enter **www.Unified CCMP.com**.
>
> - For deployments with a single internal address (including load-balanced deployments) enter the part of the address after **https://**. For example, if your internal address is **https://Unified CCMP.intranet.local**, enter**Unified CCMP.intranet.local**
>
> - For deployments where the web servers will be accessed directly with no load-balancing, enter the fully qualified domain name of the server being configured. For example, **webserver1.mydomain.com**.

- To *request an external certificate*:

  - In the **Actions** pane, select **Create Certificate Request** to display the **Request Certificate** dialog box.

  - In the **Common Name** field, enter the application domain name as defined above.

- Complete the other fields as appropriate, and click **Next**.
- In the **Cryptographic Service Provider Properties** dialog box leave the default settings and click **Next**.
- Specify a file name for the certificate, and then click **Finish**.
- When you receive the certificate from the certificate authority, repeat step 1. and step 2. above to show the Server Certificates and Action panes, and in the **Action** pane, select **Complete Certificate Request.**
- Enter the file name of the certificate, and a Friendly Name of your choice and click **OK**.

- To *generate an internal certificate*:
  - Select **Create Domain Certificate** in the **Actions** pane to display the **Distinguished Name Properties** dialog box.
  - In the **Common Name** field, enter the application domain name as defined above.
  - Complete the other fields as appropriate, and click **Next**.
  - In the **Online Certification Authority** dialog box specify the **Online Authority** and **a Friendly Name**. Click **Finish.**

6.2.3   Export the Certificate in PFX Format

To export the certificate in PFX format:

1. In **IIS Manager**, select the **Features View** tab, and in the **IIS** group, click on **Server Certificates**.

2. Select the certificate in the **Actions** pane and click **Export**.

3. In the **Export Certificate** dialog box, do the following:

   a. Either type a file name in the **Export to** box or click **Browse** and specify the file in which to store the exported certificate.

   b. If you want to protect the exported certificate with a password, enter a password in the **Password** box, and repeat the same password in the **Confirm** password box.

   c. Click **OK**. The certificate is exported as a PFX file.

6.2.4   Configure SSL for the Web Application

To configure SSL for the web application:

1. In a web browser, navigate to **https://<web-address>/SSLConfig**, where **<web-address>** is the web address of your Unified CCMP deployment. For example, if your web address is **https://Unified CCMP.intranet.local**, enter **https://Unified CCMP.intranet.local/SSLConfig**.

2. In the authentication dialog box, enter the username and password of a Windows domain user with administrator rights on the domain.

3. On the **SSL Certificate Configuration** page, click **Choose File** and browse to the PFX file you created in the previous section. Click **Open** to select the file.

4. If the PFX file is password-protected, enter the password in **Password**. If not, leave Password blank.

5. Click **Upload** to start the SSL configuration. When the SSL configuration is complete, the following message is shown:

    SSL Configuration Complete.

6.3   Bind Server Ports to IPv6 Addresses

The server ports that will be used for http and https communications must be bound to IPv6 addresses only. To do this, on the App/Web server:

1. In **IIS Manager** expand the **Sites** node and select **Default ;Web Site**. Under **Actions**, select **Bindings**.

2. Select **http** and click **Edit**. In the IP Address field enter **[::1]**. Click **OK**.

3. Select **https** and click **Edit**. In the IP Address field select the IPv6 address assigned to the App/Web server. In the SSL certificate field, select the SSL certificate that has the fully qualified domain name installed on the server.

4. Click **OK**, then **Close**.

5. At the command prompt, enter **iisreset**.

6.4   Configure Antivirus Options

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

*   The folders containing the database files (***.ldf**, ***.mdf** and ***.ndf**) on the Database Server. To locate these files, start **SQL Management Studio**, expand the **Databases** node, and select **Properties** for the database. If you

selected the default database name at installation, the database will be **Portal**. In the Database Properties dialog box, select the **Files** page to see the folder and file names of the database files.

* The Importer folder on the Database Server. If you selected the default installation location, this will be **C:\Program Files\Management Portal\Data Import Server\IMPORTER**.

* The Web folder and all subfolders on the App/Web Server. If you selected the default installation location, this will be **C:\Program Files\Management Portal\Web**.

6.5 Performance Tuning Checklists

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

6.5.1 Web Servers

Description	Done
Create a new page file, on a non-system drive, specifying the option to allow Windows to manage the page file size.	
Defragment the page file and registry hives using **http://www.sysinternals.com/Utilities/PageDefrag.html**.	

6.5.2 Database Servers

Description	Done
Create a new page file, on a non-system drive, specifying the option to allow Windows to manage the page file size.	
Defragment page file and registry hives using **http://www.sysinternals.com/Utilities/PageDefrag.html**.	
Ensure the Portal database is set to **Simple Recovery Mode** on all systems.	

6.5.3 Database Servers - Additional Actions for Deployments with More Than 8,000 Agents

For deployments with more than 8,000 agents you should also do the following steps on all database servers.

Description	Done
Restrict SQL Server memory usage as follows: 1. In SQL Server Management Studio, right-click the database server, select **Properties** and go to the **Memory** page. 2. Set **Minimum server memory** to **4096** MB (4 GB) and **Maximum server memory** to **11264** MB (11 GB). 3. Click **Save** to apply the setting then close SSMS.	
Increase the Data Importer SQL command timeout as follows: 1. In Windows Explorer locate the Data Importer configuration file. If you have used the default installation location this will be at **C:\Program Files\Management Portal\Data Import Server\DataPipelineService.exe.config**. 2. Open this file in Notepad or another text editor. 3. Search for name="SqlCommandTimeout" and in the <value> tag that follows, change the time from 00:00:30 to 00:01:30. 4. Save the file. 5. Stop and restart the **UCCMP: Data Importer** windows service.	

After the initial import has completed following a new installation or upgrade, update the database statistics to improve query performance.
1. In SQL Server Management Studio, click **New Query** and enter the following:
 	
    USE Portal;
    GO
    EXEC sp_updatestats;
    GO
 	
2. Close SSMS.	

6.6 Final Post-Installation Actions

6.6.1 Restart the System

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

6.6.2 Log in to Unified CCMP

Launch **Management Portal**. This will open a web page, which you can bookmark.

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

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

6.6.3   Verify the Installation

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

1.   Log in to the Unified CCMP web application using the pre-configured **administrator** user and confirm that the Unified CCMP home page successfully displays.

2.   On each Unified CCMP server, in the **Run** command dialog box, enter **Services.msc**. Check that all the installed Unified CCMP services have been started.

3.   Use the following SQL statement to confirm that resource data is being imported to the database:

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

This query should return a value of at least 3.

6.6.4   Configure Single Sign-On (if Required)

6.6.4.1   About Single Sign-On

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

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

6.6.4.2   Set Up Administrator Account

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

1. Login to Unified CCMP as **administrator**.

2. In **User Manager**, create a user account to be the new administrator account as follows:

    •   The login name must correspond to an existing Windows Active Directory user,and must be formatted as **<username>@<domain-name>**, where **<username>** is the Windows username and **<domain-name>** is the fully qualified Windows domain name. An example is **user1@testdomain.local**. The login name must exactly match the details in the corresponding Active Directory entry.

    •   The password should conform to the password security specified in System Settings, but will never be used.

    > **Note**
    >
    > The old down-level logon name format (**<DOMAIN>\<your domain login>**) can still be also but it is recommended that all new Unified CCMP SSO users use the UPN format above.

3. Click **New User** and open **Groups** tab.

4. Click **Add to Group**.

5. Select the check box for the **Administrators** group.

6. Close and save.

6.6.4.3   Configure SSO Authentication

To configure SSO for Unified CCMP, on the Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

    •   **Server Name**. Enter the name of the primary database server.

    •   **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

    •   **Authentication**. Select Windows Authentication.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. In the **Tools** drop-down, select **System Properties**. The System Properties tool is displayed.

4. In the **Global** properties tab, locate the **Login Authentication Configuration** group, **Login Authentication Mode** property.

5. Using the drop-down beside the property value, change the value from **Portal** to **Active Directory**.

6. Click **Save** to save the configuration change, then **Exit**.

7. On the App/Web Server, go to the location where Unified CCMP was installed (usually **C:\Program Files\Management Portal**), right-click the **Web** folder and select **Properties**.

8. Select the **Security** tab, and ensure that all domain users have **Read** and **Read & Execute** permissions on this folder.

9. Click **Advanced** and ensure that **Include inheritable permissions from this object's parent** is selected. If this option is not selected, click **Change Permissions**, select it, and click **OK**.

10. Click **OK** to close the properties dialog.

11. From a command window, execute the **iisreset** command.

> **Note**
>
> The next step is only required if you have multiple additional web URLs configured to access your Unified CCMP system.

12. Log in to the domain controller as a user with administrator access to the domain. Enter the following command on the command line, where `<custom-address>` is the custom address in the additional web URL and `<Unified CCMP-webserver-name>` is the name of your Unified CCMP App/Web Server. If you have a load-balanced system, `<Unified CCMP-webserver-name>` must be the name of the load-balanced node, not the name of any of the individual servers.

    `setspn -a http/<custom-address> <Unified CCMP-webserver-name>`

    For example, if your web URL for the Unified CCMP web application is `https://mycompany/portal` and the name of your Unified CCMP App/Web Server is `Unified CCMPWeb1`, you would enter

    `setspn -a http/mycompany Unified CCMPWeb1`

    Reboot the Unified CCMP App/Web Server or servers.

You have now configured SSO and users will be able to access Unified CCMP directly from their domain account without needing to log in again.

> **Note**
>
> Depending on the way that Active Directory is configured in your installation, you may also need to change additional properties in the **Login Authentication Configuration** group in ICE System Properties. The default settings will be sufficient for most installations, but in some cases, you may need to change one or both of **Active Directory Binding Options** and **Active Directory Context Type** properties too.
>
> For more information about the **Active Directory Binding Options** and **Active Directory Context Type** properties, see the *Administration Guide for Cisco Unified Contact Center Management Portal*. For information about the values to choose for your Active Directory configuration, consult your Windows system administrator.

6.6.4.4 Manage Users with Single Sign-On

Once SSO has been set up, any existing Unified CCMP user accounts will no longer be valid. Login names for new users should be in the **<username>@<domain-name>** format, for example,**user1@testdomain.local**.

For more information about creating Unified CCMP user accounts, see the *User Guide for Cisco Unified Contact Center Management Portal*, Security Manager section.

7   Upgrading From a Previous Version

7.1   About the Upgrade Procedure

7.1.1   General Information

This chapter describes how to upgrade from Unified CCMP 9.0 or later. For information about upgrading from an earlier version, please contact your vendor support.

> **Note**
>
> This version of Unified CCMP requires Windows Server 2012 R2 and SQL Server 2014. Earlier versions of Unified CCMP used Windows Server 2008 and SQL Server 2008. Before upgrading from Unified CCMP 10.5(1) or earlier, the servers must be completely rebuilt. In-situ upgrades are not supported. You can either prepare new servers running Windows Server 2012, or you can rebuild your existing servers.

7.1.2   Upgrade Options

The upgrade procedure for Unified CCMP depends on your deployment model, and your requirements for the upgrade. For example, upgrading a single server system is simpler than upgrading a resilient two-tier system where down-time must be minimized. You should choose the method that best suits your system configuration and upgrade requirements.

This table lists the different upgrade procedures and the scenarios where they can be used.

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

7.1.3   More About Upgrading Dual-Sided Systems

Unified CCMP employs a distributed architecture for dual-sided systems. Resilience is achieved by the use of a second side of the system containing the same components as the primary side. SQL Server replication is used to replicate data from Side A to Side B and Side B to Side A.

Failover information for the individual Unified CCMP components is stored in the databases on Side A and B. This information is also replicated using SQL Server replication. This means that both sides have knowledge of the primary and secondary server configuration made through the Unified CCMP Integrated Configuration Management tool, even when replication has been removed.
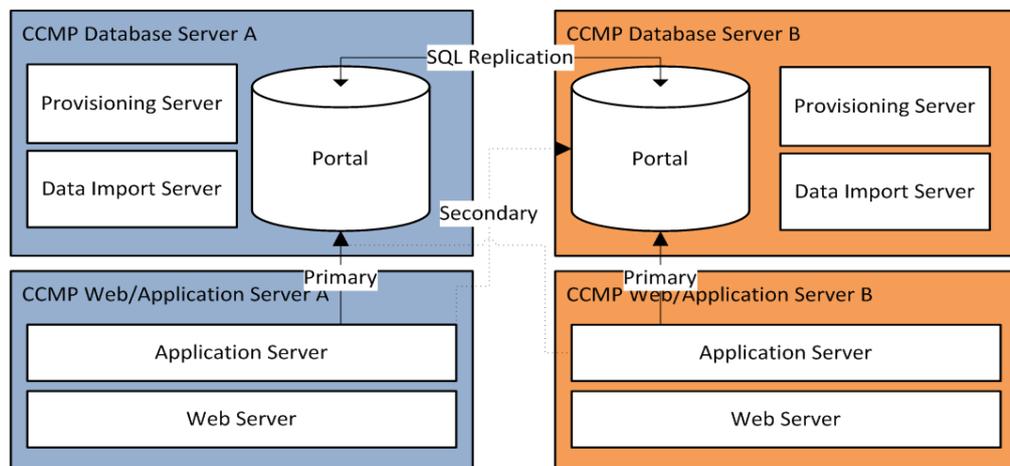
Figure 7.1   Replication and Failover Connections

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

There are two ways to upgrade dual-sided systems:

- If it is acceptable for the system to be completely unavailable whilst the upgrade is performed, then use the Total Outage Upgrade method. This is the quicker upgrade method.

- If high-availability is required, then use the Split-Sided Upgrade method. This method maximizes the system up time during the upgrade but adds additional complexity.

7.2   Validating an Upgrade

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

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

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

8   Single-Sided Upgrade

8.1   About a Single-Sided Upgrade

This chapter describes the steps involved to upgrade a single-sided deployment. The description assumes that you have a two tier deployment (separate database and app/web servers), although you can still use these instructions if you have an all-in-one installation.

Warning!

Ensure that you have up-to-date backups of all Unified CCMP databases before you begin the upgrade. Instructions for doing this are included here.

Note

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

8.2   Checklist for Single-Sided Upgrades

Step	Complete
Prepare to upgrade	
Stop the Unified CCMP Services	
Backup the Unified CCMP portal database	
Configure new windows servers	
Create user accounts	
Apply optional security configuration	

Step	Complete
Install SQL Server and restore database	
Install and configure SQL Server	
Restore the portal database	
Add network service accounts	
Upgrade and configure Unified CCMP components	
Install the Database Installer	
Upgrade the portal database	
Install the App/Web Server	
Reconfigure the Unified CCMP servers	
Reconfigure the Unified CCE Servers	
Reconfigure Unified CCE to use new servers	
Post-installation actions	
Restart and Validate	
Restart the Unified CCMP services	
Validate the upgrade	

8.3   Prepare to Upgrade

8.3.1   Stop the Unified CCMP Services

Before starting the upgrade, you must stop all Unified CCMP services on all servers.

Stop the Unified CCMP Database Server Services

On the Database Server:

1.   In **services.msc**, stop the **UCCMP: Data Import Server** service.

2.   Repeat this step for the UCCMP**: Partitioning Table Manager** service.

3.   Repeat this step for the UCCMP**: Provisioning Server** service.

Stop the Unified CCMP App/Web Server Services

On the App/Web Server:

1. In **services.msc**, stop the **UCCMP: System Monitoring Services** service.

2. If you see a prompt saying that all other services will stop, and asking you if you want to continue, select **Yes**.

3. If there are any other running Unified CCMP services, stop them too.

8.3.2   Back up the Portal Database

Back up the Portal database and copy the backup to a safe location where it can be accessed once the latest version of Unified CCMP has been installed on the new servers.

To back up the Portal database, on the Database Server:

1. Launch **SQL Server Management Studio**.

2. Navigate to the Portal database.

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

4. Close SQL Server Management Studio.

8.3.3   Configure New Windows Servers

On the new servers running Windows Server 2012 R2, apply the Windows post-installation configuration in section 3.1 "Windows Configuration".

8.3.4   Create User Accounts

Create the SQL Agent User account as described in section 3.3 "User Accounts"

8.3.5   Apply Optional Security Configuration

On the new servers running Windows Server 2012 R2, apply the security settings described in section 3.4 "Optional Security Configuration"

8.4   Install SQL Server and Restore Database

8.4.1   Install and Configure SQL Server

On the Database Server:

1. Install SQL Server 2014 as described in section 3.2.1 "Install SQL Server".

2. Configure the SQL Server network protocols as described in section 3.2.2 "Configure SQL Server Network Protocols".

3. Configure the Windows Firewall for SQL Server as described in section 3.2.3 "Configure Windows Firewall for SQL Server".

8.4.2   Restore the Portal Database

Restore the portal database from the backup you made earlier.

On the Database Server:

1. Launch **SQL Server Management Studio**.

2. Right-click the **Databases** folder and click **Restore Database**.

3. In the Restore Database window choose **From Device**, click **Add** and add the location of the database back up file you want to restore from. You may need to copy the backup file to a local file in order to access it. Click **OK**.

4. Select the check box next to the backup set you just added.

5. From the **To Database** drop-down list, select the **Portal** database as the restore destination.

6. Select **Options** and choose **Overwrite the existing database**. This will restore the database to the same location as the previous database. If you would like to choose a different location, update the **Restore As** path for each file to your preferred data file location.

7. Click **OK** to start the restore.

8.4.3   Add Network Service Accounts

You must add the NETWORK SERVICE account for all web servers to the database logins with appropriate access permissions. Before this can be done the existing accounts must be deleted from the Portal database logins.

On the Database Server:

1. Launch **SQL Server Management Studio** and in the Object Explorer, expand the **Portal** database. A list of folders is displayed.

2. Expand the **Portal > Security > Users** folder. A list of database logins is displayed.

3. For each occurrence of the **NETWORK SERVICE** account for a remote web server in the deployment, right-click it and select **Delete**.

> **Note**
>
> Do not delete the entry for the NETWORK SERVICE account for the local machine (**NT AUTHORITY\NETWORK SERVICE**).

> The NETWORK SERVICE logins for remote web server machines in the deployment are of the form **<DOMAIN>\<WEBSERVER MACHINE NAME>$**. For example, if your web server is called **WEBSERVERA** and belongs to the **UCCMPDOM** domain, the NETWORK SERVICE login would be **UCCMP\WEBSERVERA$**.

4. In the Object Explorer, expand the top-level **Security** folder. A list of folders is displayed.

5. Right-click the **Logins** folder and select **New Login**.

6. Ensure the **Windows authentication** option is selected and enter the NT AUTHORITY\NETWORK SERVICE account for the Side A web server in the form **<DOMAIN>\<WEBSERVER MACHINE NAME>$.**

7. In the **Select a page** pane on the left hand side, click **User Mapping**.

8. In the **Users mapped to this login** section, select the **Portal** database.

9. Ensure that the User column correctly contains the Network Service account for the web server.

10. In the **Database Role Membership** section, select the **portalapp** role, **portalrs** role and **portalreporting** role.

11. Click **OK**.

12. For deployments with multiple web servers, repeat step 5. to step 11. for each additional web server.

8.5   Upgrade and Configure Unified CCMP Components

8.5.1   Install the Database Installer

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

On the Database Server:

1. Insert the Unified CCMP DVD and start the Unified CCMP Installer (for more information about the Unified CCMP Installer, see section 4.2.1 "About the Unified CCMP Installer").

2. Select **Database Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.

3. When all checks have passed, click **Install**. At this point, the Informix client is installed first if necessary. If you see the Informix client installation screen, click **Install**.

4. When the Informix client has been installed, the installation of the Database Installer starts, and the **Setup** window displays.

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

6. In the **License Agreement** window:

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

7. In the **Cryptography Configuration** window:

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

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

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

8. In the **Configure Database** window:

    • **Database Name**. Enter the name of the database catalog for Unified CCMP. By default this is **Portal**.

    • **Connect Using**. Select the login credentials you want to use:

        • **Windows Authentication Credentials of Application**. This is the recommended option.

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

    • Click **Next**.

9. In the **Destination Folder** window, if you want to change the location where the database components are stored, click **Change** and select the new location. It is not necessary to install all Unified CCMP components in the same location.

10. Click **Install** to install the Database Installer. During this process, the J2SE prerequisite will be automatically installed if it is not already present. If this happens, follow the screen prompts to complete the J2SE installation. If you see a Security Alert dialog box during the installation, saying 'Revocation Information for the security certificate for this site is not available', click **Yes** to continue.

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

12. Click **Finish**.

8.5.2   Upgrade the Portal Database

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

On the Database Server:

1. If you selected the Launch Database Management Utility check box when you installed the Database Installer, the Database Installer starts automatically after it has been installed. Otherwise, launch Unified CCMP **Database Installer**. The Database Installer is a wizard which guides you through the steps to upgrade the database.

2. Click **Next** to begin the upgrade process.

3. In the Database Setup Window choose **Upgrade an Existing Database**. Click **Next** to continue.

4. In the SQL Server Connection Details window, take the following actions:

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

    • **Database Name**. Enter or select the name of the database catalog that was originally used for the Unified CCMP database.

    • **Connect Using**. Select the login credentials you want to use:

        • The **Windows account information you use to log in to your computer**. This is the recommended option.

- The **Microsoft SQL Server login information assigned by the system administrator**. Only select this option if you are using a database catalog on a different domain. For this option you must enter your Login Name and Password in the fields provided.

- **Test Connection**. Click to make sure the connection to the Microsoft SQL Server is established. If you see the message 'Connection succeeded but database does not exist' then you must rectify this problem before continuing. Check that the database catalog name and security credentials are correct.

- When the database connection details have been tested and the connection is successful, click **Next**.

5. Click **Next** to perform the upgrade. The upgrade may take several minutes.

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

8.5.3   Install the App/Web Server

On the App/Web Server:

1. Insert the Unified CCMP DVD and start the Unified CCMP Installer (for more information about the Unified CCMP Installer, see section 4.2.1 "About the Unified CCMP Installer").

2. Select **App/Web Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.

3. When all checks have passed, click **Install** to begin the App/Web Server installation. The **Management Portal: Application Server Components** window displays.

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

5. If the Management Portal: Application Server Components Dialog is displayed, click **Install** to install the additional required components.

6. If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.5 Framework is complete, restart the server to continue the installation of the App/Web Server.

7. In the **License Agreement** window:

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

8. In the **Cryptography Configuration** window:

- **Passphrase**. Enter the cryptographic passphrase you used for the installation of the Database Server component.

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

- Click **Next** to continue.

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

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

10. In the **Configure Database** window:

- **SQL Server Name**. Enter the host name or IP Address of the server hosting the Unified CCMP database. The default name of **localhost** is only valid if you are installing this component on the Database Server. Otherwise, specify the name of the Database Server. For a dual-sided deployment enter the name of the Side A Database server when installing the Side A components and enter the name of the Side B Database Server when installing the Side B components.

- **Catalog Name**. Enter or select the database catalog name you specified when installing the Database Server component. If you used the default value, this will be **Portal**.

- **Connect Using**. Select the login credentials you want to use:

  - **Windows authentication.** This is the recommended option.

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

- Click **Next** to continue.

11. Click **Install**.

12. When the installation has completed, click **Finish**. When installation is complete, the machine will restart.

8.5.4   Reconfigure the Unified CCMP Servers

> **Note**
>
> This step is only required if you have reinstalled Unified CCMP on new servers with different names. This step is not required if you have upgraded your existing servers, or have replaced your existing servers with new servers with the same names.

If the Unified CCMP server names have changed, the Unified CCMP cluster configuration must be updated to reference the new server names.

To update the cluster configuration, on the Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

   - **Server Name**. Enter the name of the primary database server.

   - **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

   - **Authentication**. Select Windows Authentication.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

> **Note**
>
> If the Unified CCMP server names have changed, several errors may be reported when ICE starts for the first time after an upgrade. The steps in this section will fix the errors.

3. Select the **Setup** tab and click **Setup UCCMP Servers** to start the wizard. Click **Next** to go through each window in turn.

4. On the various **Configure Servers** pages, change the existing server name for each of the Unified CCMP servers to the new server name. The number of pages and servers to specify will depend on your deployment type. On each page, enter the following, then click **Next**:

   - **Primary Server**

     - **Server Name**. This is the non-domain qualified machine name.

     - **Server Address**. This defaults to Server Name. This can be changed to an IP Address or a domain qualified name of the server.

   - **Secondary Server**:

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

5. Click **Next** and enter the relevant server information for each Unified CCMP server until you reach one of the following pages: **Primary Database Administrator Login**, **Secondary Database Administrator Login** or **Configure Relational Database Connection**.

6. Click **Next** to go through the remaining windows in turn, without changing anything.

7. When you see the confirmation message indicating that the wizard has completed successfully, click **Exit** to close the wizard.

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

9. In **ICE**, select the **Servers** tab. The list of servers will show both the old servers and the new servers. Right-click each of the old servers and select **Remove Server**.

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

8.5.5   Reconfigure the Unified CCE Servers

Note

This step is only required if you have upgraded Unified CCE at the same time as upgrading Unified CCMP. This step is not required if you have not upgraded Unified CCE.

If you have upgraded Unified CCE at the same time upgrading Unified CCMP, the Unified CCMP cluster must be updated to ensure that Unified CCMP can communicate with Unified CCE. It may also be necessary to configure the Unified CCE Config Web Service, which wasn't present in some earlier versions of Unified CCE.

To reconfigure the Unified CCE servers after Unified CCE has been upgraded, on the Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

   - **Server Name**. Enter the name of the primary database server.

   - **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

   - **Authentication**. Select Windows Authentication.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. Select the **Setup** tab and click **Configure Cisco Unified CCE Servers** to start the wizard.

4. On the **Select Task** page, select **Modify an existing instance**. Select the Unified CCE instance that has been updated, and click **Next** to go through each page in turn.

5. If you see the **Configure Primary Unified Config Web Service** page, enter or confirm the following details

    *   **URL**. This is the auto-generated URL of the primary Unified Config Web Service on the Unified CCE.

    *   **User Name**. This is a username with appropriate access to the Unified CCE that the web service is running on. This user must be in the domain security group **<Server>_<UCCE-Instance>_Config**, where *<Server>* is the name of the server running Unified CCE and *<UCCE-Instance>* is the name of the Unified CCE Instance on this server.

    *   **Password**. This is the password for the user.

6. If you see the **Configure Primary ConAPI RMI Ports** page, enter or confirm the following ConAPI details:

    *   **Local Registry Port**. This is the port on the Unified CCE for the Unified CCMP Provisioning service to connect to. This will usually be 2099.

    *   **Remote Registry Port**. This is the port on the Unified CCMP Database Server for the Unified CCE to connect to. This will usually be 2099.

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

7. If you see the **Configure ConAPI Application Instance** page enter the following details:

    *   **Application Name.** The name of the application to be used for provisioning Unified CCE from Unified CCMP. Specify the name of the application you configured in section 5.3.2 "Set Up ConAPI".

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

8.   On the **Multi Media Support** page, if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance to provide support for non-voice interactions, select **Yes**. The default is No.

9.   On the **Purge On Delete** page, if you want to purge items from Unified CCE automatically when they are deleted from Unified CCMP, select **Yes**. The default is Yes.

10.   On the **Supervisor Active Directory Integration** page, if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors, select **Yes**. The default is No. If you select Yes, you will be prompted to provide Active Directory information so that Windows user accounts can be listed.

11.   The Summary dialog box summarizes the details of the Unified CCE being configured and the settings you have chosen. Check the details, and if you are satisfied, click **Next**.

12.   A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.

13.   For each remaining Unified CCE Server that has been upgraded, click **Configure Cisco Unified CCE Servers**, and repeat the steps above.

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

8.5.6   Reconfigure Unified CCE to Use the New Servers

> **Note**
>
> This step is only required if you have reinstalled Unified CCMP on new servers with different names. This step is not required if you have upgraded your existing servers, or have replaced your existing servers with new servers with the same names.

If you have reinstalled Unified CCMP on new servers with different names, Unified CCE must be updated to reference the new Unified CCMP servers.

To do this, on each Unified CCE instance in your deployment:

1.   Launch **CMS Control**. This opens the CMS control console.

2.   On the **Application** tab, select the Unified CCMP database server and click **Edit**.

3.   In the **Application connection details** tab, change the existing server name to the new server name. There are three places where this needs to be done:

- **Administration & Data Server Link**. The name of the newUnified CCMP Database Server, in capital letters, with **Server** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBServer**.

- **Application link**. The name of the new Unified CCMP Database Server, in capital letters, with **Client** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBClient**.

- **Application host name**. The name of the new Unified CCMP Database Server, in capital letters, for example, **PRODUCTDB**.

4. **Click** OK, then **OK** again to save the changes and exit CMS Control.

8.6   Post-Upgrade Actions

After you have upgraded Unified CCMP, complete the following post-installation steps:

- configure SSL as described in section 6.2 "Configure SSL"

- bind server ports to IPv6 addresses as described in section section 6.3 "Bind Server Ports to IPv6 Addresses"

- configure anti-virus operations as described in section 6.4 "Configure Antivirus Options"

- implement the performance tuning steps described in section 6.5 " Performance Tuning Checklists"

- complete the final post-installation actions described in section 6.6 "Final Post-Installation Actions"

> **Note**
> If your installation uses single sign-on, the configuration is restored when the database is restored, so you do not need to reconfigure single sign-on as described in section 6.6.4 "Configure Single Sign-On (if Required)"

8.7   Restart and Validate

8.7.1   Restart the Unified CCMP Services

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

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

1. In the **Run** command dialog box, enter **Services.msc** and click **OK**.

2. For each Unified CCMP service listed:

    - if the selected service is in the Started state, right click the service name and click **Restart**

    - if the selected service is not started, right-click the service name and click **Start**.

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

8.7.2   Validate the Upgrade

Check that the system is functional following the upgrade using the validation tests in section 7.2 "Validating an Upgrade".

9   Total Outage Upgrade

9.1   About a Total Outage Upgrade

This chapter describes the steps involved to upgrade a dual-sided deployment, where all servers will be taken down and upgraded at once. The description assumes that you have a two tier deployment (separate database and app/web servers) although you can still use these instructions if you have an all-in-one installation.

Warning!

Ensure that you have up-to-date backups of all Unified CCMP databases before you begin the upgrade. Instructions for doing this are included here.

Note

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

9.2   Checklist for Total Outage Upgrades

Step	Complete
Prepare to upgrade	
Stop the Unified CCMP services	
Remove database replication	
Backup the Unified CCMP portal databases	
Configure new windows servers	

Step	Complete
Create user accounts	
Apply optional security configuration	
Install SQL Server and restore database	
Install and configure SQL Server	
Restore the portal database	
Configure the SQL Agent user	
Add network service accounts	
Upgrade and configure Unified CCMP components	
Install the Database Installer	
Upgrade the portal database	
Install Database Installer and Upgrade portal database (Side B)	
Install the App/Web Server	
Reconfigure the Unified CCMP servers	
Reconfigure the Unified CCE Servers	
Reconfigure Unified CCE to use new servers	
Restore Replication	
Configure Replication	
Monitor the replication snapshot	
Post-upgrade actions	
Restart and validate	
Restart the Unified CCMP services	
Validate the upgrade	

9.3 Prepare to Upgrade

9.3.1 Stop the Unified CCMP Services

Before starting the upgrade, you must stop all Unified CCMP services on all servers.

Stop the Unified CCMP Database Server Services

On the Side A Database Server:

1.   In **services.msc**, stop the **UCCMP: Data Import Server** service.

2.   Repeat this step for the UCCMP**: Partitioning Table Manager** service.

3.   Repeat this step for the UCCMP**: Provisioning Server** service.

Repeat these steps on the Side B Database Server.

Stop the Unified CCMP App/Web Server Services

On the Side A App/Web Server:

1.   In **services.msc**, stop the **UCCMP: System Monitoring Services** service.

2.   If you see a prompt saying that all other services will stop, and asking you if you want to continue, select **Yes**.

3.   If there are any other running Unified CCMP services, stop them too.

Repeat these steps on the Side B App/Web Server.

9.3.2   Remove Database Replication

Before you can upgrade a dual-sided system, database replication must be removed.

To remove database replication:

1.   Ensure you are logged in to the Side A Database Server as a domain level user with administrative rights over both Database Servers.

2.   Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

     •   **Server Name**. Enter the name of the primary database server.

     •   **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

     •   **Authentication**. Select Windows Authentication.

3.   Click **OK**. The ICE Cluster Configuration tool starts by default.

4.   From the Tool drop-down list select **Replication Manager**.

5.   Click the **Setup** tab to see the replication setup details.

6.   Click **Disable** to remove replication from the Unified CCMP database. When prompted, click **Yes** to proceed with replication removal.

7.   Replication removal may take several minutes. Wait for the 'Replication Removed' message to display in the Output Window and then exit ICE.

9.3.3   Back up the Portal Database

Back up the Portal database and copy the backup to a safe location where it can be accessed once the latest version of Unified CCMP has been installed on the new servers.

To back up the Portal database, on the Side A Database Server:

1.   Launch **SQL Server Management Studio**.

2.   Navigate to the Portal database.

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

4.   Close SQL Server Management Studio.

Repeat these steps on the Side B Database Server.

9.3.4   Configure New Windows Servers

On the new Side A and Side B servers running Windows Server 2012 R2, apply the Windows post-installation configuration in section 3.1 "Windows Configuration".

9.3.5   Create User Accounts

Create the SQL Agent User account as described in section 3.3 "User Accounts"

9.3.6   Apply Optional Security Configuration

On the new Side A and Side B servers running Windows Server 2012 R2, apply the security settings described in section 3.4 "Optional Security Configuration"

9.4   Install SQL Server and Restore the Database

9.4.1   Install and Configure SQL Server

On the Side A Database Server:

1.   Install SQL Server 2014 as described in section 3.2.1 "Install SQL Server".

2.   Configure the SQL Server network protocols as described in section 3.2.2 "Configure SQL Server Network Protocols".

3.   Configure the Windows Firewall for SQL Server as described in section 3.2.3 "Configure Windows Firewall for SQL Server".

Repeat these steps on the Side B Database Server.

9.4.2 Restore the Portal Database

Restore the Side A portal database from the Side A backup you made earlier.

On the Side A Database Server:

1. Launch **SQL Server Management Studio**.

2. Right-click the **Databases** folder and click **Restore Database**.

3. In the Restore Database window choose **From Device**, click **Add** and add the location of the database back up file you want to restore from. You may need to copy the backup file to a local file in order to access it. Click **OK**.

4. Select the check box next to the backup set you just added.

5. From the **To Database** drop-down list, select the **Portal** database as the restore destination.

6. Select **Options** and choose **Overwrite the existing database**. This will restore the database to the same location as the previous database. If you would like to choose a different location, update the **Restore As** path for each file to your preferred data file location.

7. Click **OK** to start the restore.

Repeat the process on the Side B Database Server to restore the Side B portal database backup to the Side B Database Server.

9.4.3 Configure the SQL Agent User

For a dual-sided system, the SQL Agent User must be reconfigured.

On the Side A Database Server:

1. Launch **SQL Server Management Studio** and expand the **Security** folder. A list of subfolders is displayed.

2. Right-click the **Logins** folder and select **New Login**.

3. Ensure the **Windows authentication** option is selected and enter the SQL Agent User domain and login name in the form **<DOMAIN>\<LOGIN>**. For example, if your user is called **sql_agent_user** and belongs to the **CISCO** domain, enter **CISCO\sql_agent_user.**

4. In the **Select a page** pane on the left hand side, click **User Mapping**.

5. In the **Users mapped to this login** section, select the **Portal** database. The User column will auto-populate with the domain username for the SQL Agent User.

6. In the **Database Role Membership** section, select the **db_owner** role.

7.   Click **OK** to apply the changes.

Repeat these steps on the Side B Database Server.

9.4.4   Add Network Service Accounts

You must add the NETWORK SERVICE account for all web servers to the database logins with appropriate access permissions. Before this can be done the existing accounts must be deleted from the Portal database logins.

On the Side A Database Server:

1.   Launch **SQL Server Management Studio** and in the Object Explorer, expand the **Portal** database. A list of folders is displayed.

2.   Expand the **Portal > Security > Users** folder. A list of database logins is displayed.

3.   For each occurrence of the **NETWORK SERVICE** account for a remote web server in the deployment, right-click it and select **Delete**.

> **Note**
>
> Do not delete the entry for the NETWORK SERVICE account for the local machine (**NT AUTHORITY\NETWORK SERVICE**).
>
> The NETWORK SERVICE logins for remote web server machines in the deployment are of the form **<DOMAIN>\<WEBSERVER MACHINE NAME>$**. For example, if your web server is called **WEBSERVERA** and belongs to the **UCCMPDOM** domain, the NETWORK SERVICE login would be **UCCMP\WEBSERVERA$**.

4.   In the Object Explorer, expand the top-level **Security** folder. A list of folders is displayed.

5.   Right-click the **Logins** folder and select **New Login**.

6.   Ensure the **Windows authentication** option is selected and enter the NT AUTHORITY\NETWORK SERVICE account for the Side A web server in the form **<DOMAIN>\<WEBSERVER MACHINE NAME>$.**

7.   In the **Select a page** pane on the left hand side, click **User Mapping**.

8.   In the **Users mapped to this login** section, select the **Portal** database.

9.   Ensure that the User column correctly contains the Network Service account for the web server.

10.   In the **Database Role Membership** section, select the **portalapp** role, **portalrs** role and **portalreporting** role.

11.   Click **OK**.

12.   For deployments with multiple web servers, repeat step 5. to step 11. for each additional web server.

Repeat these steps on the Side B Database Server.

9.5   Upgrade and Configure Unified CCMP Components

9.5.1   Install the Database Installer

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

On the Side A Database Server:

1.   Insert the Unified CCMP DVD and start the Unified CCMP Installer (for more information about the Unified CCMP Installer, see section 4.2.1 "About the Unified CCMP Installer").

2.   Select **Database Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.

3.   When all checks have passed, click **Install**. At this point, the Informix client is installed first if necessary. If you see the Informix client installation screen, click **Install**.

4.   When the Informix client has been installed, the installation of the Database Installer starts, and the **Setup** window displays.

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

6.   In the **License Agreement** window:

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

7.   In the **Cryptography Configuration** window:

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

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

   Warning!

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

8. In the **Configure Database** window:

    - **Database Name**. Enter the name of the database catalog for Unified CCMP. By default this is **Portal**.

    - **Connect Using**. Select the login credentials you want to use:

        - **Windows Authentication Credentials of Application**. This is the recommended option.

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

    - Click **Next**.

9. In the **Destination Folder** window, if you want to change the location where the database components are stored, click **Change** and select the new location. It is not necessary to install all Unified CCMP components in the same location.

10. Click **Install** to install the Database Installer. During this process, the J2SE prerequisite will be automatically installed if it is not already present. If this happens, follow the screen prompts to complete the J2SE installation. If you see a Security Alert dialog box during the installation, saying 'Revocation Information for the security certificate for this site is not available', click **Yes** to continue.

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

12. Click **Finish**.

9.5.2   Upgrade the Portal Database

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

On the Side A Database Server:

1. If you selected the Launch Database Management Utility check box when you installed the Database Installer, the Database Installer starts automatically after it has been installed. Otherwise, launch Unified CCMP **Database Installer**. The Database Installer is a wizard which guides you through the steps to upgrade the database.

2. Click **Next** to begin the upgrade process.

3. In the Database Setup Window choose **Upgrade an Existing Database**. Click **Next** to continue.

4. In the SQL Server Connection Details window, take the following actions:

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

    •   **Database Name**. Enter or select the name of the database catalog that was originally used for the Unified CCMP database.

    •   **Connect Using**. Select the login credentials you want to use:

        •   The **Windows account information you use to log in to your computer**. This is the recommended option.

        •   The **Microsoft SQL Server login information assigned by the system administrator**. Only select this option if you are using a database catalog on a different domain. For this option you must enter your Login Name and Password in the fields provided.

    •   **Test Connection**. Click to make sure the connection to the Microsoft SQL Server is established. If you see the message 'Connection succeeded but database does not exist' then you must rectify this problem before continuing. Check that the database catalog name and security credentials are correct.

    •   When the database connection details have been tested and the connection is successful, click **Next**.

5. Click **Next** to perform the upgrade. The upgrade may take several minutes.

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

9.5.3   Install Database Installer and Upgrade Portal Database (Side B)

On the Side B Database Server:

1. Install the Database Installer as described in section 9.5.1 "Install the Database Installer".

2.   Upgrade the Portal database as described in section 9.5.2 "Upgrade the Portal Database".

9.5.4   Install the App/Web Server

On the Side A App/Web Server:

1.   Insert the Unified CCMP DVD and start the Unified CCMP Installer (for more information about the Unified CCMP Installer, see section 4.2.1 "About the Unified CCMP Installer").

2.   Select **App/Web Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.

3.   When all checks have passed, click **Install** to begin the App/Web Server installation. The **Management Portal: Application Server Components** window displays.

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

5.   If the Management Portal: Application Server Components Dialog is displayed, click **Install** to install the additional required components.

6.   If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.5 Framework is complete, restart the server to continue the installation of the App/Web Server.

7.   In the **License Agreement** window:

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

8.   In the **Cryptography Configuration** window:

•   **Passphrase**. Enter the cryptographic passphrase you used for the installation of the Database Server component.

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

•   Click **Next** to continue.

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

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

10.   In the **Configure Database** window:

- **SQL Server Name**. Enter the host name or IP Address of the server hosting the Unified CCMP database. The default name of **localhost** is only valid if you are installing this component on the Database Server. Otherwise, specify the name of the Database Server. For a dual-sided deployment enter the name of the Side A Database server when installing the Side A components and enter the name of the Side B Database Server when installing the Side B components.

- **Catalog Name**. Enter or select the database catalog name you specified when installing the Database Server component. If you used the default value, this will be **Portal**.

- **Connect Using**. Select the login credentials you want to use:

  - **Windows authentication.** This is the recommended option.

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

- Click **Next** to continue.

11.   Click **Install**.

12.   When the installation has completed, click **Finish**. When installation is complete, the machine will restart.

Repeat these steps on the Side B App/Web Server.

9.5.5 Reconfigure the Unified CCMP Servers

> **Note**
>
> This step is only required if you have reinstalled Unified CCMP on new servers with different names. This step is not required if you have upgraded your existing servers, or have replaced your existing servers with new servers with the same names.

If the Unified CCMP server names have changed, the Unified CCMP cluster configuration must be updated to reference the new server names.

This only needs to be done on the Side A Database Server. The Side B servers will be updated when replication is reinstated. To update the cluster configuration, on the Side A Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

    *   **Server Name**. Enter the name of the primary database server.

    *   **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

    *   **Authentication**. Select Windows Authentication.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

    > **Note**
    >
    > If the Unified CCMP server names have changed, several errors may be reported when ICE starts for the first time after an upgrade. The steps in this section will fix the errors.

3. Select the **Setup** tab and click **Setup UCCMP Servers** to start the wizard. Click **Next** to go through each window in turn.

4. On the various **Configure Servers** pages, change the existing server name for each of the Unified CCMP servers to the new server name. The number of pages and servers to specify will depend on your deployment type. On each page, enter the following, then click **Next**:

    *   **Primary Server**

        *   **Server Name**. This is the non-domain qualified machine name.

        *   **Server Address**. This defaults to Server Name. This can be changed to an IP Address or a domain qualified name of the server.

- **Secondary Server**:

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

5. Click **Next** and enter the relevant server information for each Unified CCMP server until you reach one of the following pages: **Primary Database Administrator Login**, **Secondary Database Administrator Login** or **Configure Relational Database Connection**.

6. Click **Next** to go through the remaining windows in turn, without changing anything.

7. When you see the confirmation message indicating that the wizard has completed successfully, click **Exit** to close the wizard.

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

9. In **ICE**, select the **Servers** tab. The list of servers will show both the old servers and the new servers. Right-click each of the old servers and select **Remove Server**.

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

These steps do not need to be repeated on the Side B Database Server as the necessary changes will be applied when replication is reinstated.

9.5.6 Reconfigure the Unified CCE Servers

> **Note**
>
> This step is only required if you have upgraded Unified CCE at the same time as upgrading Unified CCMP. This step is not required if you have not upgraded Unified CCE.

If you have upgraded Unified CCE at the same time upgrading Unified CCMP, the Unified CCMP cluster must be updated to ensure that Unified CCMP can communicate with Unified CCE. It may also be necessary to configure the Unified CCE Config Web Service, which wasn't present in some earlier versions of Unified CCE.

This only needs to be done on Side A. Side B will be updated when replication is reinstated. To reconfigure the Unified CCE servers after Unified CCE has been upgraded, on the Side A Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

   - **Server Name**. Enter the name of the primary database server.

- **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

- **Authentication**. Select Windows Authentication.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. Select the **Setup** tab and click **Configure Cisco Unified CCE Servers** to start the wizard.

4. On the **Select Task** page, select **Modify an existing instance**. Select the Unified CCE instance that has been updated, and click **Next** to go through each page in turn.

5. If you see the **Configure Primary Unified Config Web Service** page, enter or confirm the following details

- **URL**. This is the auto-generated URL of the primary Unified Config Web Service on the Unified CCE.

- **User Name**. This is a username with appropriate access to the Unified CCE that the web service is running on. This user must be in the domain security group **<Server>_<UCCE-Instance>_Config**, where *<Server>* is the name of the server running Unified CCE and *<UCCE-Instance>* is the name of the Unified CCE Instance on this server.

- **Password**. This is the password for the user.

6. If you see the **Configure Primary ConAPI RMI Ports** page, enter or confirm the following ConAPI details:

- **Local Registry Port**. This is the port on the Unified CCE for the Unified CCMP Provisioning service to connect to. This will usually be 2099.

- **Remote Registry Port**. This is the port on the Unified CCMP Database Server for the Unified CCE to connect to. This will usually be 2099.

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

7. If you see the **Configure ConAPI Application Instance** page enter the following details:

- **Application Name.** The name of the application to be used for provisioning Unified CCE from Unified CCMP. Specify the name of the application you configured in section 5.3.2 "Set Up ConAPI".

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

8. On the **Multi Media Support** page, if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance to provide support for non-voice interactions, select **Yes**. The default is No.

9. On the **Purge On Delete** page, if you want to purge items from Unified CCE automatically when they are deleted from Unified CCMP, select **Yes**. The default is Yes.

10. On the **Supervisor Active Directory Integration** page, if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors, select **Yes**. The default is No. If you select Yes, you will be prompted to provide Active Directory information so that Windows user accounts can be listed.

11. The Summary dialog box summarizes the details of the Unified CCE being configured and the settings you have chosen. Check the details, and if you are satisfied, click **Next**.

12. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.

13. For each remaining Unified CCE Server that has been upgraded, click **Configure Cisco Unified CCE Servers**, and repeat the steps above.

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

These steps do not need to be repeated on the Side B Database Server as the necessary changes will be applied when replication is reinstated.

9.5.7   Reconfigure Unified CCE to Use the New Servers

> **Note**
>
> This step is only required if you have reinstalled Unified CCMP on new servers with different names. This step is not required if you have upgraded your existing servers, or have replaced your existing servers with new servers with the same names.

If you have reinstalled Unified CCMP on new servers with different names, Unified CCE must be updated to reference the new Unified CCMP servers.

To do this, on each Unified CCE instance in your Side A deployment:

1. Launch **CMS Control**. This opens the CMS control console.

2. On the **Application** tab, select the Unified CCMP database server and click **Edit**.

3. In the **Application connection details** tab, change the existing server name to the new server name. There are three places where this needs to be done:

   - **Administration & Data Server Link**. The name of the newUnified CCMP Database Server, in capital letters, with **Server** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBServer**.

   - **Application link**. The name of the new Unified CCMP Database Server, in capital letters, with **Client** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBClient**.

   - **Application host name**. The name of the new Unified CCMP Database Server, in capital letters, for example, **PRODUCTDB**.

4. **Click** OK, then **OK** again to save the changes and exit CMS Control.

Repeat these steps on each Unified CCE instance in your Side B deployment.

9.6　　Restore Replication

9.6.1　　Configure Replication

Replication between the databases is set up and monitored using the Replication Manager application which is available in the Unified CCMP Integrated Configuration Environment (ICE) tool.

> **Note**
>
> The user running Replication Manager must have administrator permissions in both Windows and SQL Server, for both the publisher and the subscriber Database Servers.
>
> Usually, the publisher will be the Side A Database Server, but occasionally, it may be necessary to configure the Side B Database Server as the publisher.

To configure replication, on the publisher Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

   - **Server Name**. Enter the name of the primary database server.

- **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

- **Authentication**. Select Windows Authentication.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. From the Tool drop-down list, select **Replication Manager**. The Replication Manager opens in the Setup tab. The Setup tab has the following sections:

   - **Unified CCMP Database Server Properties** contains the publisher and subscriber Unified CCMP database details.

   - **Distributor Properties** contains the SQL Server Replication distributor properties.

   The default values shown in the Setup tab are derived from the values initially configured in the Cluster Configuration tool and will be suitable in most cases.

4. If required, modify the Unified CCMP Database Server Properties.

   - **Server Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.

   - **Catalog Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration. It may be changed, but if so, a valid database with the new name must already exist on the corresponding server.

5. If required, modify the distributor properties.

   - **Server Name**. The name of the subscriber server hosting the Unified CCMP database. This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.

   - **Catalog Name**. The name to be assigned to the distribution database. The recommended value is **distribution_portal**.

   - **Data Folder**. The folder path on the distributor server where the data file for the distribution database will be created.

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

- **Log Folder**. The folder path on the distributor server where the transaction log file for the distribution database will be created.

- **Distribution Share**. The distribution share folder where replication snapshot files will be generated.

- **Override Distributor Admin Password**. Select to override the auto-generated replication password which will be used to establish connectivity. The auto-generated password is 14 characters long, and will contain alpha-numeric characters (both upper and lower case) and a special character. If this does not meet the complexity requirements of the server then select this option and specify a password of your choice.

6. When you have set the required replication properties, click **Configure** to configure replication.

7. You may be prompted to save pending changes to the database before continuing. If so, click **Yes** to save pending changes and continue.

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

9.6.2   Monitor the Replication Snapshot

Note

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

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

To monitor the progress of the replication snapshot:

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

- **Publications** (top left) lists the publisher servers and the publications on each publisher that need to be shared with the subscribers.

- **Subscriptions and Agents** (top right) shows the subscriptions to a publication and the replication agents associated with a publication. This pane has two tabs, Subscriptions and Agents.

- **Subscriptions** shows the subscriptions to the selected publication. You can right-click on a subscription to start or stop the subscription.

- **Agents** shows the replication agents associated with the selected publication. You can right-click on a replication agent to start or stop the agent.

- **Sessions** (bottom left) shows all sessions for the selected publication and replication agent in the last 24 hours.

- **Actions** (bottom right) shows the activity for the selected session.

2. In the top left hand pane, select the first Unified CCMP database publication from the list of publications. If you have used the default database name, this will start with **[Portal]**.

3. Wait for the replication snapshot for this publication to complete.

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

   "Delivered snapshot from . . . "

   "No replicated transactions are available".

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

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

4. Repeat the two steps above for each of the remaining Unified CCMP database publications.

5. When replication is complete for all portal database publications, close the ICE tool.

The subscriber database can now be used to service requests. For more information about the Replication Manager see the *Integrated Configuration Environment (ICE) for Cisco Unified Contact Center Management Portal*.

9.7 Post-Upgrade Actions

After you have upgraded Unified CCMP, complete the following post-installation steps:

- configure SSL as described in section 6.2 "Configure SSL"

- bind server ports to IPv6 addresses as described in section section 6.3 "Bind Server Ports to IPv6 Addresses"

- configure anti-virus operations as described in section 6.4 "Configure Antivirus Options"

- implement the performance tuning steps described in section 6.5 " Performance Tuning Checklists"

- complete the final post-installation actions described in section 6.6 "Final Post-Installation Actions"

Note

If your installation uses single sign-on, the configuration is restored when the database is restored, so you do not need to reconfigure single sign-on as described in section 6.6.4 "Configure Single Sign-On (if Required)"

9.8 Restart and Validate

9.8.1 Restart the Unified CCMP Services

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

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

1. In the **Run** command dialog box, enter **Services.msc** and click **OK**.

2. For each Unified CCMP service listed:

   - if the selected service is in the Started state, right click the service name and click **Restart**

   - if the selected service is not started, right-click the service name and click **Start**.

Note

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

9.8.2 Validate the Upgrade

Check that the system is functional following the upgrade using the validation tests in section 7.2 "Validating an Upgrade".

10   Split Sided Upgrade

10.1   About a Split Sided Upgrade

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

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

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

This process has two parts.

- Part 1 - split the dual-sided system and upgrade Side A (see section 10.2 "Checklist for Split Side Upgrades (Side A)").

- Part 2 - upgrade Side B and restore replication (see section 10.8 "Checklist for Split Side Upgrades (Side B)").

There are two options for restoring the Side B database. They are:

- **Option 1**. Restore the Side B database from the Side B backup taken before the upgrade, then upgrade the restored database. This is the recommended method if the system has been running in single-sided mode for less than 24 hours.

- **Option 2**. Restore the Side B database from the upgraded Side A database. In this case, you will not need to upgrade the database after you have restored it. This is the recommended method if the system has been running in single-sided mode for more than 24 hours.

The description assumes that you have a two tier deployment (separate database and app/web servers) although you can still use these instructions if you have an all-in-one installation.

> **Warning!**
> Ensure that you have up-to-date backups of all Unified CCMP databases before you begin the upgrade. Instructions for doing this are included here.

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

10.2 Checklist for Split Side Upgrades (Side A)

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

Step	Complete
Prepare to upgrade	
Stop the Unified CCMP services	
Force failover connections to Side B	
Update Side B to enable provisioning and import (optional)	
Remove database replication	
Backup the Unified CCMP portal databases	
Configure new windows servers	
Create user accounts	
Apply optional security configuration	
Install SQL Server and restore database	
Install and configure SQL Server (Side A)	

Step	Complete
Restore the portal database (Side A)	
Configure the SQL Agent user (Side A)	
Add network service accounts (Side A)	
Upgrade and configure Unified CCMP components (Side A)	
Install the Database Installer	
Upgrade the portal database	
Install the App/Web Server	
Reconfigure the Unified CCMP servers	
Reconfigure the Unified CCE Servers	
Reconfigure Unified CCE to use new servers	
Post-upgrade actions	
Restart and validate (Side A)	
Restart the Unified CCMP services	
Validate the upgrade	

10.3   Prepare to Upgrade (Side A)

10.3.1   Stop the Unified CCMP Services

Before starting the upgrade, you must stop all Unified CCMP services on all servers.

Stop the Unified CCMP Database Server Services

On the Side A Database Server:

1.   In **services.msc**, stop the **UCCMP: Data Import Server** service.

2.   Repeat this step for the UCCMP**: Partitioning Table Manager** service.

3.   Repeat this step for the UCCMP**: Provisioning Server** service.

Stop the Unified CCMP App/Web Server Services

On the Side A App/Web Server:

1.   In **services.msc**, stop the **UCCMP: System Monitoring Services** service.

2. If you see a prompt saying that all other services will stop, and asking you if you want to continue, select **Yes**.

3. If there are any other running Unified CCMP services, stop them too.

10.3.2   Force Failover Connections to the Active Side

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

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

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

DBA

```
127.0.0.1              DBB
```

DBB

```
127.0.0.1              DBA
```

WEBA

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

WEBB

```
<IP ADDRESS OF DBB>    DBA
 127.0.0. 1            WEBA
```
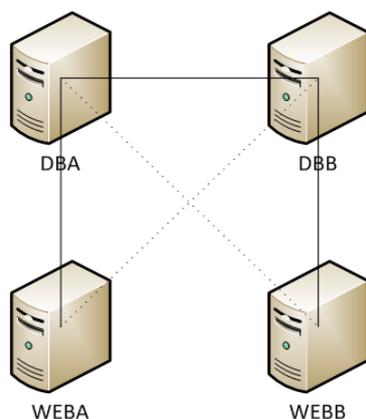
Figure 10.1   Host File Entries For Failover in Single-sided Mode

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

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

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

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

10.3.4   Remove Database Replication

Before you can upgrade a dual-sided system, database replication must be removed.

To remove database replication:

1.   Ensure you are logged in to the Side A Database Server as a domain level user with administrative rights over both Database Servers.

2.   Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

     •   **Server Name**. Enter the name of the primary database server.

- **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

- **Authentication**. Select Windows Authentication.

3. Click **OK**. The ICE Cluster Configuration tool starts by default.

4. From the Tool drop-down list select **Replication Manager**.

5. Click the **Setup** tab to see the replication setup details.

6. Click **Disable** to remove replication from the Unified CCMP database. When prompted, click **Yes** to proceed with replication removal.

7. Replication removal may take several minutes. Wait for the 'Replication Removed' message to display in the Output Window and then exit ICE.

10.3.5   Back up the Portal Database

Back up the Portal database and copy the backup to a safe location where it can be accessed once the latest version of Unified CCMP has been installed on the new servers.

To back up the Portal database, on the Side A Database Server:

1. Launch **SQL Server Management Studio**.

2. Navigate to the Portal database.

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

4. Close SQL Server Management Studio.

10.3.6   Configure New Windows Servers

On the new Side A servers running Windows Server 2012 R2, apply the Windows post-installation configuration in section 3.1 "Windows Configuration".

10.3.7   Create User Accounts

Create the SQL Agent User account as described in section 3.3 "User Accounts"

10.3.8   Apply Optional Security Configuration

On the new Side A servers running Windows Server 2012 R2, apply the security settings described in section 3.4 "Optional Security Configuration"

10.4   Install SQL Server and Restore the Portal Database (Side A)

10.4.1   Install and Configure SQL Server (Side A)

On the Side A Database Server:

1.   Install SQL Server 2014 as described in section 3.2.1 "Install SQL Server".

2.   Configure the SQL Server network protocols as described in section 3.2.2 "Configure SQL Server Network Protocols".

3.   Configure the Windows Firewall for SQL Server as described in section 3.2.3 "Configure Windows Firewall for SQL Server".

10.4.2   Restore the Portal Database (Side A)

Restore the Side A portal database from the Side A backup you made earlier.

On the Side A Database Server:

1.   Launch **SQL Server Management Studio**.

2.   Right-click the **Databases** folder and click **Restore Database**.

3.   In the Restore Database window choose **From Device**, click **Add** and add the location of the database back up file you want to restore from. You may need to copy the backup file to a local file in order to access it. Click **OK**.

4.   Select the check box next to the backup set you just added.

5.   From the **To Database** drop-down list, select the **Portal** database as the restore destination.

6.   Select **Options** and choose **Overwrite the existing database**. This will restore the database to the same location as the previous database. If you would like to choose a different location, update the **Restore As** path for each file to your preferred data file location.

7.   Click **OK** to start the restore.

10.4.3   Configure the SQL Agent User (Side A)

For a dual-sided system, the SQL Agent User must be reconfigured.

On the Side A Database Server:

1.   Launch **SQL Server Management Studio** and expand the **Security** folder. A list of subfolders is displayed.

2.   Right-click the **Logins** folder and select **New Login**.

3. Ensure the **Windows authentication** option is selected and enter the SQL Agent User domain and login name in the form **<DOMAIN>\<LOGIN>**. For example, if your user is called **sql_agent_user** and belongs to the **CISCO** domain, enter **CISCO\sql_agent_user.**

4. In the **Select a page** pane on the left hand side, click **User Mapping**.

5. In the **Users mapped to this login** section, select the **Portal** database. The User column will auto-populate with the domain username for the SQL Agent User.

6. In the **Database Role Membership** section, select the **db_owner** role.

7. Click **OK** to apply the changes.

10.4.4   Add Network Service Accounts (Side A)

You must add the NETWORK SERVICE account for all web servers to the database logins with appropriate access permissions. Before this can be done the existing accounts must be deleted from the Portal database logins.

On the Side A Database Server:

1. Launch **SQL Server Management Studio** and in the Object Explorer, expand the **Portal** database. A list of folders is displayed.

2. Expand the **Portal > Security > Users** folder. A list of database logins is displayed.

3. For each occurrence of the **NETWORK SERVICE** account for a remote web server in the deployment, right-click it and select **Delete**.

> **Note**
>
> Do not delete the entry for the NETWORK SERVICE account for the local machine (**NT AUTHORITY\NETWORK SERVICE**).
>
> The NETWORK SERVICE logins for remote web server machines in the deployment are of the form **<DOMAIN>\<WEBSERVER MACHINE NAME>$**. For example, if your web server is called **WEBSERVERA** and belongs to the **UCCMPDOM** domain, the NETWORK SERVICE login would be **UCCMP\WEBSERVERA$**.

4. In the Object Explorer, expand the top-level **Security** folder. A list of folders is displayed.

5. Right-click the **Logins** folder and select **New Login**.

6. Ensure the **Windows authentication** option is selected and enter the NT AUTHORITY\NETWORK SERVICE account for the Side A web server in the form **<DOMAIN>\<WEBSERVER MACHINE NAME>$.**

7. In the **Select a page** pane on the left hand side, click **User Mapping**.

8. In the **Users mapped to this login** section, select the **Portal** database.

9. Ensure that the User column correctly contains the Network Service account for the web server.

10. In the **Database Role Membership** section, select the **portalapp** role, **portalrs** role and **portalreporting** role.

11. Click **OK**.

12. For deployments with multiple web servers, repeat step 5. to step 11. for each additional web server.

10.5 Upgrade and Configure Unified CCMP Components - Side A

10.5.1 Install the Database Installer

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

On the Side A Database Server:

1. Insert the Unified CCMP DVD and start the Unified CCMP Installer (for more information about the Unified CCMP Installer, see section 4.2.1 "About the Unified CCMP Installer").

2. Select **Database Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.

3. When all checks have passed, click **Install**. At this point, the Informix client is installed first if necessary. If you see the Informix client installation screen, click **Install**.

4. When the Informix client has been installed, the installation of the Database Installer starts, and the **Setup** window displays.

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

6. In the **License Agreement** window:

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

7. In the **Cryptography Configuration** window:

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

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

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

8. In the **Configure Database** window:

    - **Database Name**. Enter the name of the database catalog for Unified CCMP. By default this is **Portal**.

    - **Connect Using**. Select the login credentials you want to use:

        - **Windows Authentication Credentials of Application**. This is the recommended option.

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

    - Click **Next**.

9. In the **Destination Folder** window, if you want to change the location where the database components are stored, click **Change** and select the new location. It is not necessary to install all Unified CCMP components in the same location.

10. Click **Install** to install the Database Installer. During this process, the J2SE prerequisite will be automatically installed if it is not already present. If this happens, follow the screen prompts to complete the J2SE installation. If you see a Security Alert dialog box during the installation, saying 'Revocation Information for the security certificate for this site is not available', click **Yes** to continue.

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

12.   Click **Finish**.

10.5.2   Upgrade the Portal Database

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

On the Side A Database Server:

1.   If you selected the Launch Database Management Utility check box when you installed the Database Installer, the Database Installer starts automatically after it has been installed. Otherwise, launch Unified CCMP **Database Installer**. The Database Installer is a wizard which guides you through the steps to upgrade the database.

2.   Click **Next** to begin the upgrade process.

3.   In the Database Setup Window choose **Upgrade an Existing Database**. Click **Next** to continue.

4.   In the SQL Server Connection Details window, take the following actions:

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

•   **Database Name**. Enter or select the name of the database catalog that was originally used for the Unified CCMP database.

•   **Connect Using**. Select the login credentials you want to use:

•   The **Windows account information you use to log in to your computer**. This is the recommended option.

•   The **Microsoft SQL Server login information assigned by the system administrator**. Only select this option if you are using a database catalog on a different domain. For this option you must enter your Login Name and Password in the fields provided.

•   **Test Connection**. Click to make sure the connection to the Microsoft SQL Server is established. If you see the message 'Connection succeeded but database does not exist' then you must rectify this problem before continuing. Check that the database catalog name and security credentials are correct.

•   When the database connection details have been tested and the connection is successful, click **Next**.

5.   Click **Next** to perform the upgrade. The upgrade may take several minutes.

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

10.5.3   Install the App/Web Server

On the Side A App/Web Server:

1. Insert the Unified CCMP DVD and start the Unified CCMP Installer (for more information about the Unified CCMP Installer, see section 4.2.1 "About the Unified CCMP Installer").

2. Select **App/Web Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.

3. When all checks have passed, click **Install** to begin the App/Web Server installation. The **Management Portal: Application Server Components** window displays.

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

5. If the Management Portal: Application Server Components Dialog is displayed, click **Install** to install the additional required components.

6. If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.5 Framework is complete, restart the server to continue the installation of the App/Web Server.

7. In the **License Agreement** window:

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

8. In the **Cryptography Configuration** window:

    •   **Passphrase**. Enter the cryptographic passphrase you used for the installation of the Database Server component.

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

    •   Click **Next** to continue.

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

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

10. In the **Configure Database** window:

   - **SQL Server Name**. Enter the host name or IP Address of the server hosting the Unified CCMP database. The default name of **localhost** is only valid if you are installing this component on the Database Server. Otherwise, specify the name of the Database Server. For a dual-sided deployment enter the name of the Side A Database server when installing the Side A components and enter the name of the Side B Database Server when installing the Side B components.

   - **Catalog Name**. Enter or select the database catalog name you specified when installing the Database Server component. If you used the default value, this will be **Portal**.

   - **Connect Using**. Select the login credentials you want to use:

      - **Windows authentication.** This is the recommended option.

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

   - Click **Next** to continue.

11. Click **Install**.

12. When the installation has completed, click **Finish**. When installation is complete, the machine will restart.

10.5.4   Reconfigure the Unified CCMP Servers

Note

This step is only required if you have reinstalled Unified CCMP on new servers with different names. This step is not required if you have upgraded your existing servers, or have replaced your existing servers with new servers with the same names.

If the Unified CCMP server names have changed, the Unified CCMP cluster configuration must be updated to reference the new server names.

To update the cluster configuration, on the Side A Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

- **Server Name**. Enter the name of the primary database server.

- **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

- **Authentication**. Select Windows Authentication.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

> **Note**
>
> If the Unified CCMP server names have changed, several errors may be reported when ICE starts for the first time after an upgrade. The steps in this section will fix the errors.

3. Select the **Setup** tab and click **Setup UCCMP Servers** to start the wizard. Click **Next** to go through each window in turn.

4. On the various **Configure Servers** pages, change the existing server name for each of the Unified CCMP servers to the new server name. The number of pages and servers to specify will depend on your deployment type. On each page, enter the following, then click **Next**:

- **Primary Server**

  - **Server Name**. This is the non-domain qualified machine name.

  - **Server Address**. This defaults to Server Name. This can be changed to an IP Address or a domain qualified name of the server.

- **Secondary Server**:

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

5. Click **Next** and enter the relevant server information for each Unified CCMP server until you reach one of the following pages: **Primary Database Administrator Login**, **Secondary Database Administrator Login** or **Configure Relational Database Connection**.

6. Click **Next** to go through the remaining windows in turn, without changing anything.

7. When you see the confirmation message indicating that the wizard has completed successfully, click **Exit** to close the wizard.

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

9. In **ICE**, select the **Servers** tab. The list of servers will show both the old servers and the new servers. Right-click each of the old servers and select **Remove Server**.

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

10.5.5   Reconfigure the Unified CCE Servers

> **Note**
>
> This step is only required if you have upgraded Unified CCE at the same time as upgrading Unified CCMP. This step is not required if you have not upgraded Unified CCE.

If you have upgraded Unified CCE at the same time upgrading Unified CCMP, the Unified CCMP cluster must be updated to ensure that Unified CCMP can communicate with Unified CCE. It may also be necessary to configure the Unified CCE Config Web Service, which wasn't present in some earlier versions of Unified CCE.

To reconfigure the Unified CCE servers after Unified CCE has been upgraded, on the Side A Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

    - **Server Name**. Enter the name of the primary database server.

    - **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

    - **Authentication**. Select Windows Authentication.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. Select the **Setup** tab and click **Configure Cisco Unified CCE Servers** to start the wizard.

4. On the **Select Task** page, select **Modify an existing instance**. Select the Unified CCE instance that has been updated, and click **Next** to go through each page in turn.

5. If you see the **Configure Primary Unified Config Web Service** page, enter or confirm the following details

    - **URL**. This is the auto-generated URL of the primary Unified Config Web Service on the Unified CCE.

- **User Name**. This is a username with appropriate access to the Unified CCE that the web service is running on. This user must be in the domain security group **<Server>_<UCCE-Instance>_Config**, where *<Server>* is the name of the server running Unified CCE and *<UCCE-Instance>* is the name of the Unified CCE Instance on this server.

- **Password**. This is the password for the user.

6. If you see the **Configure Primary ConAPI RMI Ports** page, enter or confirm the following ConAPI details:

    - **Local Registry Port**. This is the port on the Unified CCE for the Unified CCMP Provisioning service to connect to. This will usually be 2099.

    - **Remote Registry Port**. This is the port on the Unified CCMP Database Server for the Unified CCE to connect to. This will usually be 2099.

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

7. If you see the **Configure ConAPI Application Instance** page enter the following details:

    - **Application Name.** The name of the application to be used for provisioning Unified CCE from Unified CCMP. Specify the name of the application you configured in section 5.3.2 "Set Up ConAPI".

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

8. On the **Multi Media Support** page, if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance to provide support for non-voice interactions, select **Yes**. The default is No.

9. On the **Purge On Delete** page, if you want to purge items from Unified CCE automatically when they are deleted from Unified CCMP, select **Yes**. The default is Yes.

10. On the **Supervisor Active Directory Integration** page, if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors, select **Yes**. The default is No. If you select Yes, you will be prompted to provide Active Directory information so that Windows user accounts can be listed.

11.   The Summary dialog box summarizes the details of the Unified CCE being configured and the settings you have chosen. Check the details, and if you are satisfied, click **Next**.

12.   A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.

13.   For each remaining Unified CCE Server that has been upgraded, click **Configure Cisco Unified CCE Servers**, and repeat the steps above.

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

10.5.6   Reconfigure Unified CCE to Use the New Servers

Note

This step is only required if you have reinstalled Unified CCMP on new servers with different names. This step is not required if you have upgraded your existing servers, or have replaced your existing servers with new servers with the same names.

If you have reinstalled Unified CCMP on new servers with different names, Unified CCE must be updated to reference the new Unified CCMP servers.

To do this, on each Unified CCE instance in your Side A deployment:

1.   Launch **CMS Control**. This opens the CMS control console.

2.   On the **Application** tab, select the Unified CCMP database server and click **Edit**.

3.   In the **Application connection details** tab, change the existing server name to the new server name. There are three places where this needs to be done:

   •   **Administration & Data Server Link**. The name of the newUnified CCMP Database Server, in capital letters, with **Server** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBServer**.

   •   **Application link**. The name of the new Unified CCMP Database Server, in capital letters, with **Client** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBClient**.

   •   **Application host name**. The name of the new Unified CCMP Database Server, in capital letters, for example, **PRODUCTDB**.

4.   **Click** OK, then **OK** again to save the changes and exit CMS Control.

10.6   Post-Upgrade Actions

After you have upgraded Unified CCMP, complete the following post-installation steps:

- configure SSL as described in section 6.2 "Configure SSL"

- bind server ports to IPv6 addresses as described in section section 6.3 "Bind Server Ports to IPv6 Addresses"

- configure anti-virus operations as described in section 6.4 "Configure Antivirus Options"

- implement the performance tuning steps described in section 6.5 " Performance Tuning Checklists"

- complete the final post-installation actions described in section 6.6 "Final Post-Installation Actions"

> **Note**
>
> If your installation uses single sign-on, the configuration is restored when the database is restored, so you do not need to reconfigure single sign-on as described in section 6.6.4 "Configure Single Sign-On (if Required)"

10.7   Restart and Validate (Side A)

10.7.1   Restart the Unified CCMP Services

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

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

1.   In the **Run** command dialog box, enter **Services.msc** and click **OK**.

2.   For each Unified CCMP service listed:

- if the selected service is in the Started state, right click the service name and click **Restart**

- if the selected service is not started, right-click the service name and click **Start**.

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

10.7.2   Validate the Upgrade

Check that the system is functional following the upgrade using the validation tests in section 7.2 "Validating an Upgrade".

10.8   Checklist for Split Side Upgrades (Side B)

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

Step	Complete
Prepare to upgrade	
Stop the Unified CCMP services	
Backup the portal databases	
Configure new windows servers	
Create user accounts	
Apply optional security configuration	
Install SQL Server and restore database	
Install and configure SQL Server (Side B)	
Restore the portal database (Side B)	
Configure the SQL Agent user (Side B)	
Add network service accounts (Side B)	
Upgrade and configure Unified CCMP components (Side B)	
Install the Database Installer	
Upgrade the portal database	
Install the App/Web Server	
Reconfigure the Unified CCMP servers	

Step	Complete
Reconfigure the Unified CCE Servers	
Reconfigure Unified CCE to use new servers	
Post-upgrade actions	
Restore Replication	
Stop forcing failover connections to the active side	
Configure Replication	
Monitor the replication snapshot	
Restart and validate	
Restart and validate (Side A)	
Restart the Unified CCMP services	
Validate the upgrade	

10.9   Prepare to Upgrade (Side B)

10.9.1   Stop the Unified CCMP Services

Before starting the upgrade, you must stop all Unified CCMP services on all servers.

Stop the Unified CCMP Database Server Services

On the Side B Database Server:

1.   In **services.msc**, stop the **UCCMP: Data Import Server** service.

2.   Repeat this step for the UCCMP**: Partitioning Table Manager** service.

3.   Repeat this step for the UCCMP**: Provisioning Server** service.

Stop the Unified CCMP App/Web Server Services

On the Side B App/Web Server:

1.   In **services.msc**, stop the **UCCMP: System Monitoring Services** service.

2.   If you see a prompt saying that all other services will stop, and asking you if you want to continue, select **Yes**.

3.   If there are any other running Unified CCMP services, stop them too.

10.9.2   Back up the Portal Database

Back up the Portal database and copy the backup to a safe location where it can be accessed once the latest version of Unified CCMP has been installed on the new servers.

Identify the database to be backed up (see section 10.1 "About a Split Sided Upgrade" for information about the options).

•   If you are planning to restore the Side B database from the existing Side B database (option 1), you need to back up the existing Side B database now. So follow these instructions on the Side B Database Server.

•   If you are planning to restore the Side B database from the upgraded Side A database (option 2), you need to back up the upgraded Side A database now. So follow these instructions on the Side A database server.

To back up the portal database, on the selected database server:

1.   Launch **SQL Server Management Studio**.

2.   Navigate to the Portal database.

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

4.   Close SQL Server Management Studio.

10.9.3   Configure New Windows Servers

On the new Side B servers running Windows Server 2012 R2, apply the Windows post-installation configuration in section 3.1 "Windows Configuration".

10.9.4   Apply Optional Security Configuration

On the new Side B servers running Windows Server 2012 R2, apply the security settings described in section 3.4 "Optional Security Configuration"

10.10   Install SQL Server and Restore the Portal Database (Side B)

10.10.1   Install and Configure SQL Server (Side B)

On the Side B Database Server:

1.   Install SQL Server 2014 as described in section 3.2.1 "Install SQL Server".

2.   Configure the SQL Server network protocols as described in section 3.2.2 "Configure SQL Server Network Protocols".

3.   Configure the Windows Firewall for SQL Server as described in section 3.2.3 "Configure Windows Firewall for SQL Server".

10.10.2   Restore the Portal Database (Side B)

Restore the Side B portal database from the database backup you made earlier (see section 10.9 "Prepare to Upgrade (Side B)"). This backup may be a backup of the existing Side B database (option 1), or it may be a backup of the upgraded Side A database (option 2), depending on your requirements. See section 10.1 "About a Split Sided Upgrade" for information about the backup and restore options for the Side B portal database.

On the Side B Database Server:

1.   Launch **SQL Server Management Studio**.

2.   Right-click the **Databases** folder and click **Restore Database**.

3.   In the Restore Database window choose **From Device**, click **Add** and add the location of the database back up file you want to restore from. You may need to copy the backup file to a local file in order to access it. Click **OK**.

4.   Select the check box next to the backup set you just added.

5.   From the **To Database** drop-down list, select the **Portal** database as the restore destination.

6.   Select **Options** and choose **Overwrite the existing database**. This will restore the database to the same location as the previous database. If you would like to choose a different location, update the **Restore As** path for each file to your preferred data file location.

7.   Click **OK** to start the restore.

10.10.3   Configure the SQL Agent User (Side B)

For a dual-sided system, the SQL Agent User must be reconfigured.

On the Side B Database Server:

1.   Launch **SQL Server Management Studio** and expand the **Security** folder. A list of subfolders is displayed.

2.   Right-click the **Logins** folder and select **New Login**.

3.   Ensure the **Windows authentication** option is selected and enter the SQL Agent User domain and login name in the form **<DOMAIN>\<LOGIN>**. For example, if your user is called **sql_agent_user** and belongs to the **CISCO** domain, enter **CISCO\sql_agent_user.**

4. In the **Select a page** pane on the left hand side, click **User Mapping**.

5. In the **Users mapped to this login** section, select the **Portal** database. The User column will auto-populate with the domain username for the SQL Agent User.

6. In the **Database Role Membership** section, select the **db_owner** role.

7. Click **OK** to apply the changes.

10.10.4   Add Network Service Accounts (Side B)

You must add the NETWORK SERVICE account for all web servers to the database logins with appropriate access permissions. Before this can be done the existing accounts must be deleted from the Portal database logins.

On the Side B Database Server:

1. Launch **SQL Server Management Studio** and in the Object Explorer, expand the **Portal** database. A list of folders is displayed.

2. Expand the **Portal > Security > Users** folder. A list of database logins is displayed.

3. For each occurrence of the **NETWORK SERVICE** account for a remote web server in the deployment, right-click it and select **Delete**.

> **Note**
>
> Do not delete the entry for the NETWORK SERVICE account for the local machine (**NT AUTHORITY\NETWORK SERVICE**).
>
> The NETWORK SERVICE logins for remote web server machines in the deployment are of the form **<DOMAIN>\<WEBSERVER MACHINE NAME>$**. For example, if your web server is called **WEBSERVERA** and belongs to the **UCCMPDOM** domain, the NETWORK SERVICE login would be **UCCMP\WEBSERVERA$**.

4. In the Object Explorer, expand the top-level **Security** folder. A list of folders is displayed.

5. Right-click the **Logins** folder and select **New Login**.

6. Ensure the **Windows authentication** option is selected and enter the NT AUTHORITY\NETWORK SERVICE account for the Side A web server in the form **<DOMAIN>\<WEBSERVER MACHINE NAME>$.**

7. In the **Select a page** pane on the left hand side, click **User Mapping**.

8. In the **Users mapped to this login** section, select the **Portal** database.

9. Ensure that the User column correctly contains the Network Service account for the web server.

10. In the **Database Role Membership** section, select the **portalapp** role, **portalrs** role and **portalreporting** role.

11. Click **OK**.

12. For deployments with multiple web servers, repeat step 5. to step 11. for each additional web server.

10.11   Upgrade and Configure Unified CCMP Components - Side B

10.11.1   Install the Database Installer

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

On the Side B Database Server:

1. Insert the Unified CCMP DVD and start the Unified CCMP Installer (for more information about the Unified CCMP Installer, see section 4.2.1 "About the Unified CCMP Installer").

2. Select **Database Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.

3. When all checks have passed, click **Install**. At this point, the Informix client is installed first if necessary. If you see the Informix client installation screen, click **Install**.

4. When the Informix client has been installed, the installation of the Database Installer starts, and the **Setup** window displays.

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

6. In the **License Agreement** window:

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

7. In the **Cryptography Configuration** window:

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

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

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

8. In the **Configure Database** window:

   • **Database Name**. Enter the name of the database catalog for Unified CCMP. By default this is **Portal**.

   • **Connect Using**. Select the login credentials you want to use:

     • **Windows Authentication Credentials of Application**. This is the recommended option.

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

   • Click **Next**.

9. In the **Destination Folder** window, if you want to change the location where the database components are stored, click **Change** and select the new location. It is not necessary to install all Unified CCMP components in the same location.

10. Click **Install** to install the Database Installer. During this process, the J2SE prerequisite will be automatically installed if it is not already present. If this happens, follow the screen prompts to complete the J2SE installation. If you see a Security Alert dialog box during the installation, saying 'Revocation Information for the security certificate for this site is not available', click **Yes** to continue.

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

12. Click **Finish**.

10.11.2   Upgrade the Portal Database

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

> **Note**
>
> This step only required if you opted to restore the Side B portal database from a backup of the old Side B database (option 1). It is not required if you restored the Side B portal database from a backup of the existing Side A database (option 2). See section 10.1 "About a Split Sided Upgrade" for information about the backup and restore options for the Side B portal database.

On the Side B Database Server:

1. If you selected the Launch Database Management Utility check box when you installed the Database Installer, the Database Installer starts automatically after it has been installed. Otherwise, launch Unified CCMP **Database Installer**. The Database Installer is a wizard which guides you through the steps to upgrade the database.

2. Click **Next** to begin the upgrade process.

3. In the Database Setup Window choose **Upgrade an Existing Database**. Click **Next** to continue.

4. In the SQL Server Connection Details window, take the following actions:

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

    *   **Database Name**. Enter or select the name of the database catalog that was originally used for the Unified CCMP database.

    *   **Connect Using**. Select the login credentials you want to use:

        *   The **Windows account information you use to log in to your computer**. This is the recommended option.

        *   The **Microsoft SQL Server login information assigned by the system administrator**. Only select this option if you are using a database catalog on a different domain. For this option you must enter your Login Name and Password in the fields provided.

    *   **Test Connection**. Click to make sure the connection to the Microsoft SQL Server is established. If you see the message 'Connection succeeded but database does not exist' then you must rectify this problem before continuing. Check that the database catalog name and security credentials are correct.

    *   When the database connection details have been tested and the connection is successful, click **Next**.

5. Click **Next** to perform the upgrade. The upgrade may take several minutes.

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

10.11.3   Install the App/Web Server

On the Side B App/Web Server:

1.   Insert the Unified CCMP DVD and start the Unified CCMP Installer (for more information about the Unified CCMP Installer, see section 4.2.1 "About the Unified CCMP Installer").

2.   Select **App/Web Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.

3.   When all checks have passed, click **Install** to begin the App/Web Server installation. The **Management Portal: Application Server Components** window displays.

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

5.   If the Management Portal: Application Server Components Dialog is displayed, click **Install** to install the additional required components.

6.   If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.5 Framework is complete, restart the server to continue the installation of the App/Web Server.

7.   In the **License Agreement** window:

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

8.   In the **Cryptography Configuration** window:

●   **Passphrase**. Enter the cryptographic passphrase you used for the installation of the Database Server component.

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

●   Click **Next** to continue.

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

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

10.   In the **Configure Database** window:

- **SQL Server Name**. Enter the host name or IP Address of the server hosting the Unified CCMP database. The default name of **localhost** is only valid if you are installing this component on the Database Server. Otherwise, specify the name of the Database Server. For a dual-sided deployment enter the name of the Side A Database server when installing the Side A components and enter the name of the Side B Database Server when installing the Side B components.

- **Catalog Name**. Enter or select the database catalog name you specified when installing the Database Server component. If you used the default value, this will be **Portal**.

- **Connect Using**. Select the login credentials you want to use:

  - **Windows authentication.** This is the recommended option.

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

- Click **Next** to continue.

11.   Click **Install**.

12.   When the installation has completed, click **Finish**. When installation is complete, the machine will restart.

10.11.4   Reconfigure the Unified CCMP Servers

> **Note**
>
> This step is only required if you have reinstalled Unified CCMP on new servers with different names. This step is not required if you have upgraded your existing servers, or have replaced your existing servers with new servers with the same names.

If the Unified CCMP server names have changed, the Unified CCMP cluster configuration must be updated to reference the new server names.

These steps are required the Side B database server, although these values will be overwritten later from the values on Side A when replication is reinstated. To update the cluster configuration, on the Side B Database Server:

1.   Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

     • **Server Name**. Enter the name of the primary database server.

     • **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

     • **Authentication**. Select Windows Authentication.

2.   Click **OK**. The ICE Cluster Configuration tool starts by default.

> **Note**
>
> If the Unified CCMP server names have changed, several errors may be reported when ICE starts for the first time after an upgrade. The steps in this section will fix the errors.

3.   Select the **Setup** tab and click **Setup UCCMP Servers** to start the wizard. Click **Next** to go through each window in turn.

4.   On the various **Configure Servers** pages, change the existing server name for each of the Unified CCMP servers to the new server name. The number of pages and servers to specify will depend on your deployment type. On each page, enter the following, then click **Next**:

     • **Primary Server**

          • **Server Name**. This is the non-domain qualified machine name.

          • **Server Address**. This defaults to Server Name. This can be changed to an IP Address or a domain qualified name of the server.

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

5. Click **Next** and enter the relevant server information for each Unified CCMP server until you reach one of the following pages: **Primary Database Administrator Login**, **Secondary Database Administrator Login** or **Configure Relational Database Connection**.

6. Click **Next** to go through the remaining windows in turn, without changing anything.

7. When you see the confirmation message indicating that the wizard has completed successfully, click **Exit** to close the wizard.

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

9. In **ICE**, select the **Servers** tab. The list of servers will show both the old servers and the new servers. Right-click each of the old servers and select **Remove Server**.

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

10.11.5   Reconfigure the Unified CCE Servers

> **Note**
>
> This step is only required if you have upgraded Unified CCE at the same time as upgrading Unified CCMP. This step is not required if you have not upgraded Unified CCE.

If you have upgraded Unified CCE at the same time upgrading Unified CCMP, the Unified CCMP cluster must be updated to ensure that Unified CCMP can communicate with Unified CCE. It may also be necessary to configure the Unified CCE Config Web Service, which wasn't present in some earlier versions of Unified CCE.

These steps are required the Side B database server, although these values will be overwritten later from the values on Side A when replication is reinstated. To reconfigure the Unified CCE servers after Unified CCE has been upgraded, on the Side B Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:
   - **Server Name**. Enter the name of the primary database server.

- **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

- **Authentication**. Select Windows Authentication.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. Select the **Setup** tab and click **Configure Cisco Unified CCE Servers** to start the wizard.

4. On the **Select Task** page, select **Modify an existing instance**. Select the Unified CCE instance that has been updated, and click **Next** to go through each page in turn.

5. If you see the **Configure Primary Unified Config Web Service** page, enter or confirm the following details

- **URL**. This is the auto-generated URL of the primary Unified Config Web Service on the Unified CCE.

- **User Name**. This is a username with appropriate access to the Unified CCE that the web service is running on. This user must be in the domain security group **<Server>_<UCCE-Instance>_Config**, where *<Server>* is the name of the server running Unified CCE and *<UCCE-Instance>* is the name of the Unified CCE Instance on this server.

- **Password**. This is the password for the user.

6. If you see the **Configure Primary ConAPI RMI Ports** page, enter or confirm the following ConAPI details:

- **Local Registry Port**. This is the port on the Unified CCE for the Unified CCMP Provisioning service to connect to. This will usually be 2099.

- **Remote Registry Port**. This is the port on the Unified CCMP Database Server for the Unified CCE to connect to. This will usually be 2099.

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

7. If you see the **Configure ConAPI Application Instance** page enter the following details:

- **Application Name.** The name of the application to be used for provisioning Unified CCE from Unified CCMP. Specify the name of the application you configured in section 5.3.2 "Set Up ConAPI".

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

8. On the **Multi Media Support** page, if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance to provide support for non-voice interactions, select **Yes**. The default is No.

9. On the **Purge On Delete** page, if you want to purge items from Unified CCE automatically when they are deleted from Unified CCMP, select **Yes**. The default is Yes.

10. On the **Supervisor Active Directory Integration** page, if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors, select **Yes**. The default is No. If you select Yes, you will be prompted to provide Active Directory information so that Windows user accounts can be listed.

11. The Summary dialog box summarizes the details of the Unified CCE being configured and the settings you have chosen. Check the details, and if you are satisfied, click **Next**.

12. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.

13. For each remaining Unified CCE Server that has been upgraded, click **Configure Cisco Unified CCE Servers**, and repeat the steps above.

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

10.11.6   Reconfigure Unified CCE to Use the New Servers

> **Note**
>
> This step is only required if you have reinstalled Unified CCMP on new servers with different names. This step is not required if you have upgraded your existing servers, or have replaced your existing servers with new servers with the same names.

If you have reinstalled Unified CCMP on new servers with different names, Unified CCE must be updated to reference the new Unified CCMP servers.

To do this, on each Unified CCE instance in your Side B deployment:

1. Launch **CMS Control**. This opens the CMS control console.

2. On the **Application** tab, select the Unified CCMP database server and click **Edit**.

3. In the **Application connection details** tab, change the existing server name to the new server name. There are three places where this needs to be done:

    • **Administration & Data Server Link**. The name of the newUnified CCMP Database Server, in capital letters, with **Server** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBServer**.

    • **Application link**. The name of the new Unified CCMP Database Server, in capital letters, with **Client** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBClient**.

    • **Application host name**. The name of the new Unified CCMP Database Server, in capital letters, for example, **PRODUCTDB**.

4. **Click** OK, then **OK** again to save the changes and exit CMS Control.

10.12 Restore Replication

10.12.1 Stop Forcing Failover Connections to the Active Side

To stop forcing the failover connections to the active side:

1. Remove the entries to the **hosts** files you made in section 10.3 "Prepare to Upgrade (Side A)".

10.12.2 Configure Replication

Replication between the databases is set up and monitored using the Replication Manager application which is available in the Unified CCMP Integrated Configuration Environment (ICE) tool.

> **Note**
>
> The user running Replication Manager must have administrator permissions in both Windows and SQL Server, for both the publisher and the subscriber Database Servers.
>
> Usually, the publisher will be the Side A Database Server, but occasionally, it may be necessary to configure the Side B Database Server as the publisher.

To configure replication, on the publisher Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

- **Server Name**. Enter the name of the primary database server.

- **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

- **Authentication**. Select Windows Authentication.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. From the Tool drop-down list, select **Replication Manager**. The Replication Manager opens in the Setup tab. The Setup tab has the following sections:

- **Unified CCMP Database Server Properties** contains the publisher and subscriber Unified CCMP database details.

- **Distributor Properties** contains the SQL Server Replication distributor properties.

The default values shown in the Setup tab are derived from the values initially configured in the Cluster Configuration tool and will be suitable in most cases.

4. If required, modify the Unified CCMP Database Server Properties.

- **Server Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.

- **Catalog Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration. It may be changed, but if so, a valid database with the new name must already exist on the corresponding server.

5. If required, modify the distributor properties.

- **Server Name**. The name of the subscriber server hosting the Unified CCMP database. This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.

- **Catalog Name**. The name to be assigned to the distribution database. The recommended value is **distribution_portal**.

- **Data Folder**. The folder path on the distributor server where the data file for the distribution database will be created.

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

- **Log Folder**. The folder path on the distributor server where the transaction log file for the distribution database will be created.

- **Distribution Share**. The distribution share folder where replication snapshot files will be generated.

- **Override Distributor Admin Password**. Select to override the auto-generated replication password which will be used to establish connectivity. The auto-generated password is 14 characters long, and will contain alpha-numeric characters (both upper and lower case) and a special character. If this does not meet the complexity requirements of the server then select this option and specify a password of your choice.

6. When you have set the required replication properties, click **Configure** to configure replication.

7. You may be prompted to save pending changes to the database before continuing. If so, click **Yes** to save pending changes and continue.

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

10.12.3   Monitor the Replication Snapshot

Note

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

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

To monitor the progress of the replication snapshot:

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

- **Publications** (top left) lists the publisher servers and the publications on each publisher that need to be shared with the subscribers.

- **Subscriptions and Agents** (top right) shows the subscriptions to a publication and the replication agents associated with a publication. This pane has two tabs, Subscriptions and Agents.

- **Subscriptions** shows the subscriptions to the selected publication. You can right-click on a subscription to start or stop the subscription.

- **Agents** shows the replication agents associated with the selected publication. You can right-click on a replication agent to start or stop the agent.

- **Sessions** (bottom left) shows all sessions for the selected publication and replication agent in the last 24 hours.

- **Actions** (bottom right) shows the activity for the selected session.

2. In the top left hand pane, select the first Unified CCMP database publication from the list of publications. If you have used the default database name, this will start with **[Portal]**.

3. Wait for the replication snapshot for this publication to complete.

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

   "Delivered snapshot from . . . "

   "No replicated transactions are available".

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

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

4. Repeat the two steps above for each of the remaining Unified CCMP database publications.

5. When replication is complete for all portal database publications, close the ICE tool.

The subscriber database can now be used to service requests. For more information about the Replication Manager see the *Integrated Configuration Environment (ICE) for Cisco Unified Contact Center Management Portal*.

10.13   Post-Upgrade Actions

After you have upgraded Unified CCMP, complete the following post-installation steps:

- configure SSL as described in section 6.2 "Configure SSL"

- bind server ports to IPv6 addresses as described in section section 6.3 "Bind Server Ports to IPv6 Addresses"

- configure anti-virus operations as described in section 6.4 "Configure Antivirus Options"

- implement the performance tuning steps described in section 6.5 " Performance Tuning Checklists"

- complete the final post-installation actions described in section 6.6 "Final Post-Installation Actions"

> **Note**
> If your installation uses single sign-on, the configuration is restored when the database is restored, so you do not need to reconfigure single sign-on as described in section 6.6.4 "Configure Single Sign-On (if Required)"

10.14   Restart and Validate (Side B)

10.14.1   Restart the Unified CCMP Services

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

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

1.   In the **Run** command dialog box, enter **Services.msc** and click **OK**.

2.   For each Unified CCMP service listed:

    - if the selected service is in the Started state, right click the service name and click **Restart**

    - if the selected service is not started, right-click the service name and click **Start**.

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

10.14.2   Validate the Upgrade

Check that the system is functional following the upgrade using the validation tests in section 7.2 "Validating an Upgrade".

11   Uninstalling Unified CCMP

11.1   About Uninstalling Unified CCMP

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

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

Uninstallation involves the following steps:

● removing database replication (dual-sided systems only)

● uninstalling the database components

● removing the database catalog (only if Unified CCMP is being removed permanently)

● uninstalling the other Unified CCMP components.

11.2   Remove Database Replication

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

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

Before removing database replication:

1. Ensure that the database is in a consistent state.

2. Stop all Unified CCMP Services on all servers.

To remove database replication:

1. Ensure you are logged in to the Side A Database Server as a domain level user with administrative rights over both Database Servers.

2. Launch **Integrated Configuration Environment** (installed as part of Unified CCMP). In the **Database Connection** dialog box, set:

    - **Server Name**. Enter the name of the primary database server.

    - **Database Name**. Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.

    - **Authentication**. Select Windows Authentication.

3. Click **OK**. The ICE Cluster Configuration tool starts by default.

4. From the Tool drop-down list select **Replication Manager**.

5. Click the **Setup** tab to see the replication setup details.

6. Click **Disable** to remove replication from the Unified CCMP database. When prompted, click **Yes** to proceed with replication removal.

7. Replication removal may take several minutes. Wait for the 'Replication Removed' message to display in the Output Window and then exit ICE.

11.3   Uninstall Application Components

To uninstall the applicationUnified CCMP components:

1. On the Side A App/Web Server, launch **Control Panel** and select **Programs and Features**.

2. Select **Management Portal: Application Server Components.**

3. Click **Uninstall.**

4. For a dual-sided deployment, repeat step 1. to step 3. on the Side B App/Web Server.

11.4   Uninstall the Database Components

To uninstall the database components, on the Database Server:

1. Launch **Control Panel** and select **Uninstall a program.**

2. Select **Management Portal: Database Components.**

3. Click **Uninstall.**

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

Note

Uninstalling the database components does not remove the Unified CCMP database catalog.

11.5   Remove the Database Catalog

Warning!

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

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

1.   Launch SQL Server Management Studio and connect to the local Database Server.

2.   In the Object Explorer pane, expand the **Databases** node, navigate to the Unified CCMP database (the default name is Portal), right click it and select **Delete**.

3.   The Delete Database window displays.

4.   Select the **Close existing connections** check box.

5.   Click **OK**.

This permanently removes the database catalog.

12   Troubleshooting

12.1   About Installer Logs

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

12.2   Changing the SQL Server Installation Language to US English

If the step to install the database installer fails with an error

Exception in installation: [SQL Server language must be US English]

you must change the SQL Server language to US English before the installation can continue. To do this, on the database server, run the following T-SQL scripts in the order below.

Script 1

```
USE master;
GO
DECLARE @LANGUAGE AS NVARCHAR(MAX);
SELECT @LANGUAGE = 'EXEC sp_configure '+CHAR(39)+'default
language'+CHAR(39)+', '+CAST([langid] AS VARCHAR(2))+';'
FROM sys.syslanguages
WHERE name = 'us_english';
EXECUTE sp_executesql @LANGUAGE;
GO
```

Script 2

```
RECONFIGURE WITH OVERRIDE;
GO
```

Script 3

```
USE [master];
ALTER LOGIN [<username>] WITH DEFAULT_LANGUAGE=[us_english];
GO
```

where *<username>* is the Windows domain user or SQL Server user you will specify for the **Connect Using** option during the installation of the Portal Database (**SQL Server Connection Details** window). For example:

- if you will connect using the option **The Windows account information I use to logon to my computer**, and have a username **user1** on **Unified CCMPDOM**, you would enter **Unified CCMPDOM\user1** for *<username>*

- if you will connect using the option **The SQL Server login information assigned by the system administrator**, and will use the **sa** user, you would enter **sa** for *<username>*.