Installation Guide
for Cisco Unified Contact Center Management Portal
Release 8.0(1)

February 2010

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

**Preface** .................................................................................................................. 1

**Purpose** .................................................................................................................. 1

**Audience** ................................................................................................................ 1

**Organization** ........................................................................................................... 1

**Obtaining Documentation, Support, and Security Guidelines** ......................... 2

**Documentation Feedback** ................................................................................... 2

1. **Cisco Unified Contact Center Management Portal** ........................................... 3

   **Overview** ............................................................................................................. 3

   **Primary Functionality** ........................................................................................ 3

   **Deployment Specifics** .......................................................................................... 4

   **Deployment Models** ............................................................................................. 5

      N-Sided Replication .............................................................................................. 5

2. **Installation Guidelines and Requirements** ...................................................... 7

   **Installation Prerequisite Checklist** .................................................................... 7

      Database ................................................................................................................. 7

      Application Server ............................................................................................... 7

      Web Server .......................................................................................................... 7

      Data Import Server ............................................................................................... 8

      Provisioning Server .............................................................................................. 8

      Diagnostic Framework ......................................................................................... 8

   **General Advice** .................................................................................................. 8

   **Server Requirements** ....................................................................................... 8

      Microsoft Windows ............................................................................................... 9

      Microsoft Microsoft SQL Server ......................................................................... 9

      Backup Guidelines .............................................................................................. 10

      Security Guidelines ............................................................................................. 10

      Reporting Services Security Configuration ......................................................... 10

   **Required User Accounts** .................................................................................. 11

      sql_agent_user .................................................................................................... 11

3. **Component Installation** .................................................................................... 12

   **Planning Your Installation** .................................................................................. 12
Security Hardening

6. Upgrading From a Previous Version
   Overview
   Uninstalling the Portal
   Uninstalling Other Components
   Upgrading Microsoft Microsoft SQL Server
   Upgrading the Portal
   Configuration

7. Platform Uninstallation
   Uninstalling Data Import Server Component
   Uninstalling the Database Component
   Uninstalling All Other Components

8. Glossary

9. Index
Preface

Purpose

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

Audience

This document is intended for System Administrators with knowledge of their Unified CCE/CCH system architecture. Microsoft SQL Server Database Administration skills are also an advantage.

Organization

Chapter 1, “Cisco Unified Contact Center Management Portal”

Introduces Unified CCMP, including its integration with Unified CCE/CCH, and how it adds value to the system. It discusses how Unified CCMP is used to configure (commission) a system deployment and to manage that system.

Chapter 2, “Installation Guidelines”

Lists the prerequisites for Unified CCMP installation and provides recommendations for pre-installation platform configuration, including platform and backup servers, antivirus software, security accounts, monitoring, system management, and data replication between servers.

Chapter 3, “Component Installation”

Provides instructions for the installation of all Unified CCMP components.

Chapter 4, “Component 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 Cluster Configuration Manager to replicate data between Database servers. Web and Database component server performance checklists are also provided.

Chapter 5, “Post Installation Steps”

Describes how to set the administrator password for, and upload report templates into, Unified CCMP platform.

Chapter 6, “Upgrading From a Previous Version”

Explains how to upgrade from an existing installation of Unified CCMP to the latest version without losing your data.

Chapter 7, “Component Uninstallation”

Describes how to remove Unified CCMP platform from your servers.
Obtaining Documentation, Support, and Security Guidelines

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


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

Documentation Feedback

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

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.
1. Cisco Unified Contact Center Management Portal

Overview

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

It simplifies the operations and procedures for performing basic tasks such as adding or modifying Agents, Skill Groups, Teams and other common administrative functions.

It provides a common web user interface to the product set. Currently, Unified CCE/CCH and Unified Communications Manager (Unified CM) use different interfaces. Simple tasks, such as adding an agent, therefore require performing multiple operations in several applications to achieve a single goal by providing a web-based unified interface for common administrative tasks, Unified CCMP decreases the amount of time, knowledge, training, and resources required to administer the solution set.

It provides an audit trail for changes made through Unified CCE/CCH. Through the supplied audit reports or the individual resource histories, administrators and other power users can trace the timing of, and the person responsible for, provisioning changes.

Unified CCE/CCH customers can optionally deploy Unified CCMP to satisfy particular business requirements.

Primary Functionality

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

- Hierarchical Administration, for example:
  - The Service Provider Administrator can add a Portal User.
  - The Tenant Administrator can add a Skill Group.
  - The Tenant Supervisor can add an Agent.

  These permissions are completely configurable.

- Audit Trails on configuration changes and usage.

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

- Commissioning consists of operations that install and initially configure a system of components. These operations are typically done by the Service Provider using existing setup and configuration tools. An example operation is setting up and configuring a peripheral.
• Provisioning consists of day-to-day configuration operations performed by a tenant. Examples include creating or modifying Agents, Skill Groups and Agent Teams.

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

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

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

Deployment Specifics

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

• Each Tenant must have its own:
  • Unified ICME/ Unified ICMH instance
  • Dedicated Administration & Data Server Real Time Distributor server. Multiple Distributor instances on a single server are not allowed.
  • Dedicated Administration & Data Server CMS Server. Multiple CMS Server instances on a single server are not allowed.
  • Unified CCMP is only supported on Unified CCE/CCH 7.1 and above, and Unified SCCE 7.5 and above.
Deployment Models

N-Sided Replication

In most deployments, Unified CCMP should be installed on a dual-sided basis to provide load balancing, resiliency, and high availability. For deployments that require layered security, such as Internet-facing environments, both sides are split across separate database servers and web/application servers by a demilitarized zone (DMZ).

Since Unified CCMP scales up with equipment and scales out with servers, a variety of cost-effective deployment models are possible. Cisco Systems recommends you read 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 an \( n \)-sided server configuration that replicates data between sites.

- **Dedicated Server.** All Unified CCMP components are installed on a single dedicated server. This system can manage 150 Portal users concurrently.

- **Secure Deployment.** Unified CCMP Application, Web, and Reporting components are hosted on one server. The Provisioning, Data Import and Database components are hosted on a second server. This system can manage 800 Portal users concurrently.
2. Installation Guidelines and Requirements

Installation Prerequisite Checklist

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

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

A summary of these prerequisites is listed below.

**Note** A Microsoft Windows Update is required for the Windows Installer (WindowsServer2003-KB898715). This must be installed prior to any installation taking place.

**Database**
- Windows Installer 3.1
- Windows Server 2003 SP2
- Microsoft .NET Framework 2.0 SP2
- Microsoft SQL Server2005 Standard or Enterprise Edition
- Microsoft SQL Server2005 SP3 including Workstation Components

**Application Server**
- Windows Installer 3.1
- Windows Server 2003 SP2
- Microsoft .NET Framework 3.5 SP1
- Microsoft SQL Server2005 SP2 Reporting Services Components
- Microsoft SQL Server2005 Workstation Components

**Web Server**
- Windows Installer 3.1
- Windows Server 2003 SP2
- Microsoft .NET Framework 2.0 SP2
- Microsoft WSE 2.0 SP3
- ASP .NET State Service 2.0 enabled
- Microsoft ASP.NET 2.0 AJAX Extensions 1.0
- Unified CCE/CCH Management Portal: Application Component
Data Import Server
- Windows Installer 3.1
- Microsoft .NET Framework 2.0 SP2
- Unified CCE/CCH Management Portal: Database Component (with database set up)

Provisioning Server
- Windows Installer 3.1
- Microsoft .NET Framework 2.0 SP2
- Unified CCE/CCH Management Portal: Database Component (with database set up)
- J2SE Runtime Environment 6.0, Update 11

Diagnostic Framework
Microsoft .NET Framework 3.5 SP1

General Advice
- Do NOT install Unified CCMP on a domain controller.
- Portal server names should consist of alphanumeric characters only, without underscores.
- Reboot the server after the installation has finished.
- The Microsoft SQL Server Agent service is required to summarize Unified CCMP audit information.
- Configure Unified CCMP to produce SNMP traps. (Please see the Administration Manual for Cisco Unified Contact Center Management Portal.)
- Norton Antivirus may state that the autorun.hta script file is malicious. If you see this message, you can safely ignore it and continue with the installation.
- Install Microsoft Internet Explorer (IE) 6 SP2 or later on all the machines from which the Management Portal website will be accessed.

Note IE 6 SP2 is not available for Microsoft Windows 2000. Any machine running this version of Microsoft Windows needs to have IE 7 or later installed.

Server Requirements
- Both the Portal servers and the Unified CCE/CCH servers should be configured to use the US English character set.
- Install Microsoft Windows 2003 Service Pack 2 on all the servers hosting the Unified CCMP.
- Install all the latest Service Packs for: Microsoft Windows 2003 (Service Pack 2), Microsoft SQL Server2005 (Service Pack 3) and Microsoft .NET v2.
- Harden the Internet Information Services Web Server (IIS) and Microsoft SQL Server2005 according to Microsoft's latest guidelines.
• Disable all unnecessary local services (FTP, BITS and so on).
• Use Microsoft Terminal Services for remote configuration and support.

**Microsoft Windows**

Once the operating system and service pack have been installed, configure the Microsoft Windows 2003 Application Server components as follows:

• Open the Configure your Server Wizard.
• In the Event Viewer, set the Application Log, Security Log and System Log to *Overwrite events as needed.*

The following components are required:

• **Microsoft Windows 2003 Application Server with ASP.NET components (IIS)** These must be selected as part of the application server configuration.
• **Microsoft .NET Framework 2.0** This is required on all servers.
• **Microsoft Script Host** Installed by default as part of Microsoft Windows 2003.

**Microsoft Microsoft SQL Server**

On the C: drive of the Database Servers install Microsoft SQL Server2005:

• When installing the Microsoft SQL Server database application, Cisco Systems recommends that you accept the default settings.
• Do not install Microsoft SQL Server as a *named instance.*
• Install Microsoft SQL Server using *mixed-mode authentication* and use *local system* for the Microsoft SQL Server and SQL Agent startup accounts.
• Allocate Microsoft SQL Server no more than 70% of the RAM in the server. Do not use dynamic RAM allocation.

Check the **Reporting Services** option during the Component Install section of the SQL setup.

Configure Reporting Services as follows:

• **Report Server Virtual Directory** Create the report server virtual directory. (The default of “ReportServer” is recommended.)
• **Report Manager Virtual Directory** Create the report manager virtual directory (the default of “Reports” is recommended).
• **Windows Service Identity** Ensure that the report server service runs under the “Local System” account.
• **Web Service Identity** Create a new application pool for the report server and manager to run in.
• **Database Connection** Create the report server database. This can be located on a different server.
• **Initialization** Ensure that your report server is initialized.
• **Email Settings** Configure your email server here to allow users to schedule reports for delivery by email in Unified CCMP.
• **Execution account** Set up an execution account for the report server to connect to an external data source. For most installations, this will be a domain account with minimum privileges. This account is required by Reporting Service when executing real-time reports through Unified CCMP.

**Backup Guidelines**

• Ensure that the Unified CCMP Portal database is set to Simple recovery mode in the database properties window of SQL Server 2005 Management Studio. Also ensure that the global Recovery Interval setting is set to 0 for the SQL Server. This setting can be configured in the Server Properties section of SQL Server 2005 Management Studio.

• Regularly back up the Microsoft SQL Server databases and truncate transaction logs to prevent them becoming excessively large.

• Schedule backups for quiet times of the day.

**Security Guidelines**

• Unified CCMP is usually deployed in an Internet facing environment. Plan security carefully before proceeding with the installation.

• The platform follows a standard web deployment model, in which web servers are deployed in a demilitarized zone (DMZ). If security is particularly important, the database servers can also be deployed in their own DMZ.

• The application should be installed while logged in using a **domain account** with **administrative** privileges over all of the platform machines.

• When installing components that require a Microsoft SQL Server Database connection you will be requested to select either Windows Authentication or Microsoft SQL Server Authentication. If you select Windows Authentication, data access will be achieved using the built-in NETWORK SERVICE account.

**Reporting Services Security Configuration**

Full privileges in Reporting Services 2005 Report Manager must be granted to the NT AUTHORITY\NETWORK SERVICE account and to the network service accounts of all the Web Application servers.

1. In Internet Explorer, open the Report Manager virtual directory on the Side A Web Application server. By default this is http://localhost/reports.

2. Click **Site Settings** from the menu at top right.

3. Under the **Security** heading, Click the **Configure site-wide security** link.

4. Click New Role Assignment.

5. Enter the NT AUTHORITY\NETWORK SERVICE user.

6. Check **System Administrator** and click **OK**.

7. Click **Home** to return to the main Report Manager page.

8. Click the **Properties** tab.

9. **Edit** the NT AUTHORITY\NETWORK SERVICE account.

10. Check all roles and click **Apply**.
Repeat this procedure for the network service accounts of all Web Application servers. These accounts are of the form `<domain name>\<machine name>`$; for example CCMPDOM\WEBAPP2$.

**Note** If accessing localhost/reports shows the header only, this may mean that anonymous access on the Reports and Reportserver virtual directories is enabled. Disable this in IIS before continuing.

**Required User Accounts**

If setting up a dual-sided replicated Management Portal installation, you need to create domain user accounts to be used by Unified CCMP. Using ActiveDirectory, create these accounts with the following attributes:

- Password never expires.
- User cannot change password.

**sql_agent_user**

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

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

Planning Your Installation

For dual-sided, or replicated, systems, perform a complete installation on the Side A server followed by a complete installation on the Side B server. Once this is completed, you can perform the configuration (including replication), as detailed in Chapter 4.

It is recommended that you install the components in the order detailed in this installation guide.

It is recommended that the Cisco Security Agent (CSA) be disabled during the installation process.

Recording Your Settings

During the installation procedure, there will be occasions where you need to record what settings you chose for later reference. Store the following information in a secure location for future reference:

<table>
<thead>
<tr>
<th>Management Portal</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Catalog Name</td>
<td></td>
</tr>
<tr>
<td>sql_agent_user</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>portal_user</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Cryptographical Passphrase</td>
<td></td>
</tr>
<tr>
<td>Administrator Password</td>
<td></td>
</tr>
<tr>
<td>CICM/ICM</td>
<td></td>
</tr>
<tr>
<td>Application Name</td>
<td></td>
</tr>
<tr>
<td>Application Key</td>
<td></td>
</tr>
<tr>
<td>Local Registry Port</td>
<td></td>
</tr>
<tr>
<td>NAM</td>
<td></td>
</tr>
<tr>
<td>Application Name</td>
<td></td>
</tr>
<tr>
<td>Application Key</td>
<td></td>
</tr>
<tr>
<td>Local Registry Port</td>
<td></td>
</tr>
</tbody>
</table>

Note: The cryptographical passphrase is a vital piece of information and must be recorded. It is used for encrypting and decrypting system passwords. It is chosen during the initial installation of the Database component and is used during the
installation of the other components and in any future installations, such as adding new servers to the cluster.

**Component Installation**

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

2. Clicking on a tab in the main panel brings up the list of prerequisites for that component and the offer to check that those prerequisites are installed.

3. It is recommended that you go through the installation of the components in the order given by this manual.

4. To begin the installation of each individual component, click its tab. Then click the Run Test… button to check that the listed prerequisite applications are installed. When the installer has verified the presence of these components, the Install button is enabled, allowing you to proceed with the installation of that component.
   
   **Note** A red cross appears next to any prerequisite application that is not installed. is displayed with a red cross next to it. This indicates that the application must be installed before the installation of the selected component can proceed. Once all the prerequisite software is installed click the Re-Run Test… button to enable the Install button.

5. When all the prerequisite applications have a green checkmark displayed next to them, click the Install button to install the chosen component.

**Database Component**

This section details how to install Unified CCMP Database server components.

**Database Component Installation**

To install Unified CCMP Database component, perform the following:

1. Select the Database Component tab, click **Run Test…** to check for prerequisites (see page 14), and click **Install**. Click **Next** to go through each window in turn.

2. On the **License Agreement** dialog window:
   
   **I accept the terms in the license agreement** You must select this option before you can continue. In doing so, you agree to be bound by the terms in the license agreement. Read it thoroughly before accepting.

3. On the **Cryptography Configuration** dialog window:
   
   **Passphrase** Create a cryptographical pass phrase of between 6 and 35 characters. This passphrase is used for encrypting and decrypting system passwords and must be the same for all servers in the cluster.
**Confirm Passphrase** You are unable to continue until the contents of this field are identical to the passphrase entered above.

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

**Caution** If you are upgrading a previous version of the Unified CCMP or adding a new server to an existing cluster, you must use the same cryptographical passphrase as was originally used. If you do not know the original passphrase, immediately cease installation and call your Support Provider. If you continue installation with a new passphrase, you will be unable to access your existing data.

4. On the **Destination Folder** window, review the location. If necessary, click **Change…** to change the location where you want the Database Server component to be installed.

5. Click **Install**.

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

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

You can also set up your database manually at a later date.

**Note** Some Management Portal components require a fully set up database in order to install.

### Database Setup

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

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

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

1. On the **SQL Server Connection Details** dialog window:
   - **Server Name** Select the Microsoft SQL Server where the Unified CCMP database should be installed. In most cases this will be the machine running the application, in which case it should be left as the default (local).
   - **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.
   - **Connect Using** Select the radio button of the login credentials you wish to apply:
     - The Windows account information I use to logon to my computer. This is the recommended option.
     - The Microsoft SQL Server login information assigned by the system administrator. This option should only be selected if you are using a
database catalog on a different domain. For this option you must enter your Login Name and Password in the fields provided.

- **Test Connection** Make sure the connection to the Microsoft SQL Server is established. The message ‘Connection succeeded but database does not exist’ is correct behavior at this point. Click OK to continue.

2. On the **Select an Action to Perform** dialog window:

- **Install a new database** Installs a new database. You may maintain or delete a database by running the installer again and selecting the appropriate option.

3. On the **Setup Replication** dialog window:

- **Replicated Configuration** Replication only needs to be configured on Side B of a dual-sided system. Check this box if this database installation is on Side B of a dual-sided, replicated system.
- **Share Name** The name of the share for the ReplData folder. By default this is ReplData.
- **Folder Path** The path of the ReplData folder. This is configured in Microsoft SQL Server. By default, it is C:\Program Files\Microsoft SQL Server\MSSQL\repldata.

4. The fields on the **Configure the Location of Data Files** dialog window only need to be completed if you are using a custom installation of Microsoft SQL Server. If you are not using a custom installation of Microsoft SQL Server, ignore these fields.

- **Location** When you select a File Group(s), its location is shown in this field. To change this location, browse to the new location.
- **Initial Size** Select the space that should be allocated for this File Group(s). The default is based on the Portal’s analysis of your system.
- **Max Size** Set the storage capacity for the selected File Group(s). You can also choose to set no limit to the file size by selecting the **Unrestricted Size** checkbox, although this is not recommended.
- **Update** Saves your changes to the selected File Group(s).
- **Default** Returns the settings for all File Groups to their default.

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

- **Account Type** The type of user account that will be used. For a distributed installation, this must be **Domain**.
- **User Name** The name of the user account. This defaults to sql_agent_user. If you used a different name when setting up the account, enter that name instead.
- **Automatically create the user account if missing** For a single sided system, it is possible to create the required user automatically. For all other systems, you must set up the required account manually. If you have not already created the user account, set it up now before continuing.
- **Password** Create a password for the new user, conforming to your individual system’s complexity requirements.
• **Confirm Password** You are unable to continue until the contents of this field are identical to the passphrase entered above.

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

7. Click **Add** to add each Web Server to the list.

8. When all Web Servers have been added, click **Next** to begin installation. Installation will take several minutes.

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

**Database Replication**
For replicated systems, repeat the installation for side B. Cisco Systems recommends that you complete side A installation before installing side B.
See Chapter 4 for details on how to perform Database replication.

**Application Server Component**
This section details how to install and configure Unified CCMP Application Server components.

**Application Server Component Installation**
To install the Unified CCMP Application Server component, select the Application Server Component tab, click **Run Test…** to check for prerequisites (see page 14), and click **Install**.
Click **Next** to go through each window in turn.

1. On the **License Agreement** dialog window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so, you agree to be bound by the terms in the license agreement. Read it thoroughly before accepting.

2. On the **Destination Folder** window, accept the folder or click **Change…** to change the location for the Application Server component.

3. On the **Cryptography Configuration** dialog window:
   - **Passphrase** Enter the Cryptographical Passphrase chosen when installing the Database component.
   - **Confirm Passphrase** You are unable to continue until the contents of this field are identical to the passphrase entered above.

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

4. On the **Cluster Configuration Database Connection** dialog window:
   - **SQL Server** Enter the name of the server where the Portal database has been installed.
     Note: The default value of the local machine is valid only for a standalone system.
   - **Catalog Name** Enter the name of the database, as selected in the Database Component installation (see page 15). By default this is Portal.
   - **Connect Using Windows authentication** should be used in most cases. If the database server is on a different network, select **Microsoft SQL Server authentication** and enter the appropriate Login ID and Password in the fields provided.

5. If performing a dual-sided installation, you are presented with the **Side B Management Portal Database Connection** dialog window.

6. Click **Install**. During the installation, command windows may be displayed while the installer configures Reporting Services. These command windows close by themselves and require no action from you.

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

**Web Server Component**

This section details how to install and configure the Unified CCMP Web Server component.

**Web Server Component Installation**

To install the Unified CCMP Web Server component, select the Web Server Component tab, click **Run Test**... to check for prerequisites (see page 14), and click **Install**.

Go through each step in turn.

1. On the **License Agreement** dialog 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.

2. Click **Install**. During the installation, command windows may be displayed while the installer configures Microsoft IIS. These command windows close by themselves and require no action from you.

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

**Data Import Server Component**

**Data Import Server Component Installation**

Note In this release, you must install the Data Import Server component on the server hosting the Database Component.
To install the Unified CCMP Data Import Server component, select the Data Import Server Component tab, click Run Test… to check for prerequisites (see page 14), and click Install.

Click Next to go through each window in turn

1. On the License Agreement dialog window:
   - I accept the terms in the license agreement You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement. Read it thoroughly before accepting.

2. On the Cryptography Configuration dialog window:
   - Passphrase Enter the cryptographical passphrase you created during installation of the Database Server component.
   - Confirm Passphrase You are unable to continue until the contents of this field are identical to the passphrase entered above.

Caution Do not dispose of the cryptographical pass phrase after installing the Data Import server component. Record this passphrase and keep it in a secure place. You will need for upgrades and during installation of Unified CCMP on new or replacement servers, and for upgrades. You will not be able to perform any of these tasks without it.

3. On the Configure Database window:
   - SQL Server Accept the default value of localhost as the server on which the database resides.
   - Catalog Name Enter the name of the database as defined during the installation of the Database Component. The default is Portal.
   - Connect Using Select Windows authentication. Microsoft SQL Server authentication is used only when connecting to a database server on a different network, which is not supported in this release.

4. On the Destination Folder window, click Change… to change the location that the Data Import Server component is installed to. It is not necessary to install all Portal components to the same location.

5. On the Session File Folder window, click Change… to change the location that temporary importer files are stored in. The default directory for these is based on the destination folder specified in the previous step.

6. Click Install.

7. When the installation is completed, click Finish.

Provisioning Server Component

Provisioning Server Component Installation

Note In this release, the Provisioning Server component must be installed on the server hosting the Database Component.

To install the Unified CCMP Provisioning component, select the Provisioning Server Component tab, click Run Test… to check for prerequisites (see page 14), and click Install.
Click **Next** to go through each window in turn.

1. On the **License Agreement** dialog window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement. Read it thoroughly before accepting.

2. On the Cryptography Configuration dialog window:
   - **Passphrase** Enter the cryptographical passphrase you created during installation of the Application Server component.
   - **Confirm Passphrase** Reenter the passphrase.
   
   **Caution** Do not dispose of the cryptographical passphrase after installing the Data Import server component. You will need it for upgrades and for installation of Unified CCMP on new or replacement servers. You will not be able to perform these tasks without it.

3. On the Configure Database dialog window:
   - **SQL Server** Select the required Microsoft SQL Server from the dropdown list. If the server you need is not listed, click Browse to specify a different server. In most cases you should accept the default of (local) for the current machine.
   - **Catalog Name** This defaults to Portal.
   - **Connect Using** Select the radio button of the login credentials you wish to apply:
     - **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 your Microsoft SQL Server Login Name and Password in the fields provided.

4. On the Destination Folder window, you can click the Change… button to change the location that the Provisioning Server component is installed to. It is not necessary to install all Unified CCMP components to the same location.

5. Click **Install**.

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

**Diagnostic Framework**

**Diagnostic Framework Installation**

**Note** In this release, the Diagnostic Framework needs to be installed on all Unified CCMP servers.

To install the Diagnostic Framework, select the Diagnostic Framework, click **Run Test**… to check for prerequisites (see page 14), and click **Install**.

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

1. On the **License Agreement** dialog window:
• **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement. Read it thoroughly before accepting.

2. On the **Destination Drive** window, you can click the **Change…** button to change the drive location that the Diagnostic Framework is installed to.

3. On the **Select Certificate** window, you can select the type of certificate in installed with the diagnostic framework. The installer will either create a Self Signed certificate or you can choose a Trusted certificate, to configure an existing certificate at a later date.

4. Click **Install**.

5. When the installation is completed, click **Finish**.
4. Component Configuration

For reasons of performance or data security, large, enterprise-wide deployments might require multiple servers to host Unified CCMP platform. Multiple platform hosts are connected together as a server cluster. This chapter details how to configure the server cluster and perform data replication. This chapter also includes performance-tuning.

The Cluster Configuration Manager is used to configure the servers that Unified CCMP will use in your deployment. Once configured, the components of Unified CCMP will be able to communicate with one another to perform such activities as Unified ICM import and Unified CCMP replication.

Before data replication between Unified CCMP databases can occur, the server(s) in the cluster must first be set up with the required prerequisite software and Unified CCMP components. Once prepared, the servers need to be assigned publisher or distributor (subscriber) roles. See Portal Databases on page 27.

Data Replication

Configuring the SQLSERVERAGENT Service

Although the Unified CCMP installer automatically grants the sql_agent_user account the necessary permissions to log on as the SQLSERVERAGENT service, it is still necessary to manually create folder shares and to check access.

To do this:

1. Log out of Windows and log in as sql_agent_user.
2. On the subscriber, locate the ReplData folder. This folder is configured in Microsoft SQL Server and by default is located in C:\Program Files\Microsoft SQL Server\MSSQL.
3. Create a share for this folder with Full Control for sql_agent_user and Local System.
4. Check that this share is accessible from the publisher while you are logged on as sql_agent_user and that you can create and delete files in it.
5. On the publisher, open the Microsoft SQL Management Studio and check connectivity to side B using Integrated Security.
6. Check that the reverse is the same (side B connectivity to side A).

Once you configure the SQLSERVERAGENT Service, log back in to both machines as the domain administrator (or as the user who installed the Management Portal if this was not the domain administrator).

You are now prepared to set up replication as part of cluster configuration.

Platform Server Cluster Configuration

This section details how to configure Unified CCMP server cluster and data replication.
The Unified CCMP Configuration Manager is an application that is used to configure server clusters, consisting of the Portal servers, Cisco Unified CCE/Unified CCH servers, and Unified CM servers that the Unified CCMP connects to. It is also used to set up replication between multiple Unified CCE/CCH Management Portal databases.

**Configuration Overview**

Before beginning cluster configuration, you must set up the ConAPI application instance and the CMS server on the Unified CCE/CCH environments.

You may then configure the server cluster. It is important to do this in the order shown.

**Note** In a replicated environment, you only run the Cluster Configuration Manager application on the **Side-A Database server**.

You need to input the list of servers, and the configuration data for each of the following in order:

- **The Portal Server(s)** – the details of the server(s) containing Unified CCMP database(s).
- **The NAM(s)** (relevant for Unified CCH only) – the details of the server(s) hosting NAM(s) and the database credentials for accessing their data.
- **The Unified CCE/CCH** – the details of the server(s) hosting Unified CCE/CCH and the database credentials for accessing their data.
- **The Unified CM(s)** – the details of the server(s) hosting the Unified CM, the endpoint and security credentials for accessing the AXL interface.

**Common ConAPI Credentials**

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

If you are using a Cisco Unified Interaction Manager installation integrated with Unified Contact Center, the Portal can be set up to use the application instance that was configured for the Cisco Unified Interaction Manager deployment. This enables you to provision non-voice skillgroups and other items through Unified CCMP. To do this, leave the **Application type** for the application instance as **Other** but change the **Permission level** to **Full read/write**. Information on configuring the application instance for a Cisco Unified Interaction Manager deployment can be found in the *Cisco Unified Web and E-Mail Interaction Manager System Administration Guide For Unified CCE/CCH Enterprise and Hosted and Unified ICM*.

To create an application instance, run Cisco Configuration Manager on the Unified ICM server as follows:

1. Open the Configuration Manager. This can normally be done from **Start > Program Files > Administration & Data Server > Configuration Manager**.
   **Note** If you are connecting to the Unified ICM server using Remote Desktop, you need to set the `/console` switch in order to run the Configuration Manager.
2. Under **Tools/List Tools** you will find the **Application Instance List**. Double-click this to open it.

3. Click the **Retrieve** button to display the list of configured application instances. To create a new application instance, click **Add**, and enter the following details:
   - **Name** A unique name to be used for the application instance.
   - **Application Key** A password to be used by the Portal to connect. This 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 **OK**.

**CMS Server Setup**

Before configuring the Unified CCMP server cluster, you must ensure that the CMS Server(s) are set up correctly on each Unified ICME/Unified ICMH/NAM AW.

**Note** Each Unified ICME/Unified ICMH requires a separate Administration & Data Server running a single instance of CMS server.

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

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

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

1. Select **Start > Run** > `C:\icm\bin\cmscontrol.exe` on the Unified ICME/Unified ICMH being configured. This opens the CMS control console.

2. Click the **Add** button to the right hand side of the window to launch the **Application Connection Details** dialog window and fill in the fields as follows:
   - **Administration & Data Server link** This should be the name of the Data Import server, in capital letters, with ‘Server’ appended, such as UCCMPServer
   - **Administration & Data Server RMI registry port** This is the port on the CICM for the Unified CCMP Provisioning server to connect to. This will usually be 2099; however if the Unified CCMP Provisioning server is connecting to multiple Unified ICME/Unified ICMH’s or the Unified ICME/Unified ICMH’s are configured as dual sided then a different port should be allocated for each Administration and Data Server.
• **Application link** This should be the name of the Data Import server, all in capital letters, with ‘Client’ appended, such as UCCMPClient.

• **Application RMI registry port** This is the port on the Provisioning Server for the Unified ICME/Unified ICMH to connect to. For convenience, this should be configured the same as for the Administration & Data Server RMI registry port.

  **Note** Each Unified ICME/Unified ICMH that the Portal will be provisioning must use a unique port. For example if Unified CCMP is configured to provision 2 dual-sided Unified ICME’s then each Unified ICME must be assigned a unique port number. This port number must be configured in the Administration & Data Server RMI registry port and in the Application RMI registry port. It will also be used later when the ConAPI connection is configured in the Unified CCMP Configuration Manager.

• **Application host name** The server name or fixed IP address, such as UCCMP or 240.24.53.107.

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

   For a dual-sided Unified CCMP system there will need to be 2 entries in the CMS control utility on each separate Administration & Data Server. These entries will refer to the side-A Unified CCMP Provisioning Server and the side-B Unified CCMP Provisioning Server.

**Configuration Procedure**

To configure Unified CCMP server cluster proceed as follows:

1. Go to **Start > All Programs > Management Portal > Configuration Manager**.

2. The **Connect to SQL Server** dialog window is displayed. On this window:

   • **Server Name** This option defaults to the current machine and cannot be changed.

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

   • **Use Integrated Security** Ensure this option is checked.

3. Click **OK** to open the **Configuration Manager**.

4. Enter the settings as described in detail below.

5. Click **Save** to save your settings, or **Revert** to cancel your changes.

   **Note** When using integrated security, the user running the **Configuration Manager** application must have permission to execute SQL on the database server on which the application is running.

The window displays the following buttons. Click a button to display the relevant configuration options.
1. Physical servers
This tab contains a list of all the servers in the cluster. Before a server is configured for a specific role such as NAM (Unified ICMH only), or Unified ICME/Unified ICMH it must be configured here.

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

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

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

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

   - **Default IP Address** Enter the IP address of the server.

2. Click **OK**.
Repeat these steps for all Unified CCMP servers, Unified ICME/Unified ICMH Servers, Unified CM Servers and NAM Servers (Unified ICMH only) in this installation.

2. UCCMP Servers

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

1. From the left-hand list of servers in the cluster, check the server which is to be the Side A Web Server.

2. Use the arrow button to move it to the **Primary Application Servers** list.

3. If there is a Side B Web Application Server, check the **Dual Sided** checkbox.

4. Select the server which is to be the Side B Web Server and move it to the **Secondary Application Servers** list.

   **Portal Databases**
This tab is used to configure the relational databases.

1. Click the **Portal Databases** tab. A table is displayed with four columns that display information about the Databases once they have been configured.

2. To add a new portal database server, click **New**. The **Portal Database Configuration** dialog window is displayed.

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

3. Enter the following details:

   - **Server** Select the server that the database is installed on from the dropdown list of the servers you configured on the **Servers** tab earlier. This defaults to the current machine.
• **Catalog** Enter the name of the database in the field provided. This defaults to Portal.

• **Default Database Connection Parameters** Select the radio button of the login credentials you wish the Database server to use.

  • **Windows authentication** Select this option only if the Local System user has administrator permissions on the server the Unified ICME/Unified ICMH is installed on, or if you have configured the Data Import Server service to run under a different user that does have administrator permissions.

  • **SQL Server authentication** Most installations should select this option. Enter the Login Name and Password in the fields provided.

    **Note** The OLAP details are not required for this version of the Management Portal.

4. Click **OK**.

Once the publisher database has been set up, you can configure replication. It is recommended that replication be configured before Unified CMs and either NAMs and Unified ICMH’s, or Unified ICME’s are added to the cluster.

**Replication**

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

2. Click the **Replicate** button (if asked to save changes, click **OK**) and confirm.

3. Click **OK** to close the UCCMP Database Replication Configuration window.

4. Click **Apply**, then **Close**.

5. Log in to the Subscriber and open the SQL Server Management Studio, then open the **Replication Monitor**. Navigate to the snapshots listed below the publisher. 2 snapshots will be displayed ([Portal] Base and [Portal] NonQueued), right-click on each snapshot in turn and select the "Reinitialize All Subscriptions" option from the list.

6. Close the SQL Server Management Studio.

**Reporting Services Servers**

This tab is used to configure the location of Reporting Services (which is a prerequisite for the Reporting Extensions component).

1. Click **New**.

2. Enter the following details:

   • **Hostname** From the drop-down list, select a server on which Reporting Services has been installed.


   • **Primary** Check this when entering the Side A server. This checkbox is disables if the Side A server has already been configured.
3. Click **Test** to check the connection.
4. Click **OK**.
5. Repeat until all servers hosting Reporting Services have been entered.

**Report Server Databases**
Configuration of Report Server Databases is not required in this version of the Management Portal.

**UCCMP Provisioning**
Use this tab to configure the location of the Provisioning Server.
1. Click **New**.
2. Enter the following details:
3. **Server** From the drop-down list, select a server on which Reporting Services has been installed.
4. Ensure the **Enabled** Checkbox is checked.
5. Click **OK**.
6. If there is a Side B Provisioning Server, repeat these steps 9 for the Side B provisioning server.

3. **Communications Servers**
This is used to configure the connection to other servers in the network.

**NAMs**
*Note* This tab is relevant to Unified CCH only.
1. Click the **NAM** tab. A table is displayed with seven columns that will show information about the NAMs once they have been configured.
2. To create a new NAM instance, click **New**. The **NAM Configuration** dialog window is displayed.
   - **Instance Name** Enter a unique name to represent the NAM instance.
   - **Server** Select the server that is hosting the NAM from the dropdown list of the servers you configured on the **Servers** tab earlier.
   - **Database Connection Parameters** Select the radio button of the login credentials you wish to apply:
     - **Windows authentication** This is the recommended option.
     - **SQL Server authentication** This option should be selected only if you are using a database catalog on a different domain. For this option you must enter your Login Name and Password in the fields provided.
     - **Unified ICMH Instance** Select the correct Unified ICMH to use from a drop-down list of those available on the selected server.
   - **HDS** In some deployments, real time and historical data may be held separately. Check this box if the specified NAM holds only historical data.
   - **AWDB Catalog** The name of the administrative workstation database catalog, such as nam_awdb. This is configured automatically.
• **HDS Catalog** The name of the historical data server catalog, such as nam_hds. This is configured automatically.

• **Common ConAPI Credentials** Set up the credentials required to connect to the NAM.
  - **Application Name** Enter the name of the application you created on the NAM earlier.
  - **Application Key** Enter the password of the application you created on the NAM earlier.
  - **Remote Registry Port** The port to connect to on the NAM. This should be 2099.
  - **Local Registry Port** This should be the same as that set up in the CMS Control Console earlier, and must be unique for each NAM.

• **Provisionable** This indicates that the NAM is to be provisioned by the Portal, and should be checked.

• **Dual Sided** Check this box if you are using a dual-sided NAM. You will then be able to fill in details for Side B.

• **Multi Media Support** Check this box if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance in order to provide support for non-voice interactions.

3. Click the **Configure Active Directory Mapping** button to open the **Browse Active Directory** dialog window. This is used to provision the domain users who are required for supervisor memberships. The domain user must be a member of the domain active directory.

  - **Domain Controller A** Enter the name of the Domain Controller.
  - **Domain Controller B** Enter the name of the Side B Domain Controller if present.
  - **Use Secure Authentication** Select this checkbox in order to login to the domain controller as a specified user.
  - **Username** Enter the name of the domain user, such as NAMSERV\administrator.
  - **Password** Enter the domain user’s password.

4. Click **Refresh**

5. Navigate to the **Active Directory** folder corresponding to the NAM instance.

6. Click **OK**, and **OK** again to save the new NAM.

**CICMs**

This is used to configure the Unified ICMEs used by Unified CCE/CCH Enterprise Edition, or the Unified ICMHs used by Unified CCE/CCH Hosted Edition. Throughout this tab, ‘Unified ICME’ refers to both Unified ICME and Unified ICMH.

1. Click the **CICM** tab. A table is displayed, with seven columns that will show information about the Unified ICME’s once they have been configured.
2. To create a new CICM instance, click **New**. The **CICM Database Configuration** dialog window is displayed.

   - **Instance Name** Enter a unique name to represent the Unified ICME in Unified CCMP.
   - **Server** Select the server that is hosting the Unified ICME from the dropdown list of the servers you configured on the **Servers** tab earlier.
   - **Database Connection Parameters** Select the radio button of the login credentials you wish to apply:
     - **Windows authentication** This is the recommended option.
     - **SQL Server authentication** This option should be selected only if you are using a database catalog on a different domain. For this option you must enter your **Login Name** and **Password** in the fields provided.
   - **ICM Instance** Select the correct Unified ICME to use from a dropdown list of those available on the selected server.
   - **HDS** In some deployments, real time and historical data may be held separately. Check this box if the specified Unified ICME holds only historical data.
   - **AWDB Catalog** The name of the administrative workstation database catalog, such as cicm_awdb. This is configured automatically.
   - **HDS Catalog** The name of the historical data server catalog, such as cicm_hds. This is configured automatically.
   - **Common ConAPI Credentials** Set up the credentials required to connect to the Unified ICME. These fields will be greyed out until the Provisionable checkbox has been checked.
     - **Application Name** Enter the name of the application you created on the Unified ICME earlier.
     - **Application Key** Enter the password of the application you created on the Unified ICME earlier.
     - **Remote Registry Port** The port to connect to on the Unified ICME. This value will default to 2099, but should be updated to the Administration & Data Server RMI Registry port configured using the Unified ICME's CMSControl tool earlier on. This port must be unique to the specific Administration & Data Server including dual-sided Unified ICME configurations.
     - **Local Registry Port** This should be the same as the Application RMI registry port set up in the CMS Control Console earlier. Where the same port number as the Remote Registry Port entered above is recommended.
     - **Local Port** This port number will be used by the Unified ICME Administration & Data Server to communicate with the Unified CCMP Provisioning Server. By default this port will be set to 3333 for Unified CCMP's A side and 3334 for Unified CCMP's B side. The local port property must be unique per Administration & Data Server. For example a dual sided installation with 2 Unified ICME's configured will have a
different local port specified for each Administration & Data Server connected to, a total number of 4 different ports.

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

3. Click the **Configure Active Directory Mapping** button. The **Browse Active Directory** dialog window is displayed. This is used to provision the domain users who are required for supervisor memberships. The domain user must be a member of the domain active directory.

- **Domain Controller A** Enter the name of the Domain Controller.
- **Domain Controller B** Enter the name of the Side B Domain Controller if present.
- **Use Secure Authentication** Select this checkbox in order to login to the domain controller as a specified user.
- **Username** Enter the name of the domain user, such as CICMSERV\administrator.
- **Password** Enter the domain user’s password.

4. Click **Refresh**.

5. Navigate to the **Active Directory** folder corresponding to the Unified ICME instance.

6. Click **OK**, and **OK** again to save the new Unified ICME.

**Unified CM s**

1. Click the **Unified CM s** tab. A table is displayed, with two columns, that will show information about the Unified CM s once they have been configured.

2. To add a Unified CM click **New**.

3. When prompted to import the Tenant/Peripheral data click **Yes**.

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

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

4. On the **Configure Unified CM** dialog window:
• **Instance Name** Enter the name to be used for the Unified CM instance by the Cluster Management utility.

**Note** For simplicity of future maintenance, it is recommended that this name be the same as the appropriate Unified ICME instance name.

• **Server** Select the server hosting the Unified CM that you configured on the Servers tab earlier.

• **Version** Select the required Unified CM version.

• **Endpoint** Enter the URL used to access the Unified CM AXL interface. The default is the default URL for the Unified CM version selected.

• **User Name** Enter the name of the Unified CM Administrator user. This is the user name that the Management Portal Data Import Server will use when connecting to the Unified CM’s web service.

• **Password** Enter the Unified CM Administrator user’s password.

• **Test** Click to test the connection to the configured Unified CM.

• **Provisionable** This indicates that the **Unified CM** is to be provisioned by the Portal, and should be checked.

5. Select the associated Unified ICME and tenants from the drop-down, and click **Add**. This will associate the Unified CM with the tenant to which it belongs.

6. Select the associated peripherals and their PG Users from the drop down and click **Add**.

• **PG User** Enter the name of a directory user on the Unified CM with whom new phones will be associated when they are created through the Unified CCMP user interface. In order for the Unified ICME to control the new phone, it must be added to a specific user’s list of controlled devices in the directory on the Unified CM. You can find a list of directory users by logging in to Cisco Unified Unified CM Administration (normally https://<SERVER>/ccmadmin, for example https://CCMSERV ccmadmin).

7. Click **OK**.

8. When you have finished adding Unified CM s, ensure the **Management Portal Data Import** service has restarted.

### 4. Connection Manager

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

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

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

The connection types are:

- **IN Datasource**
- Unified ICME /NAM AWDB
- Unified ICME /NAM HDS
• Unified CM

The **Connections by Server** tab is not relevant to this version of the Management Portal.

5. **Global Properties**

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

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

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

**Save / Revert**

Click **Save** to save your configuration or **Revert** to cancel all changes made since your last save. You might wish to view a summary of the configuration data before saving.

**View Configuration Summary**

Click the **View** menu option to see a summary of the configuration data entered, which shows the servers that make up each side of a dual-sided system.

**Import/Export Configuration**

Once the cluster has been configured, it is possible to save the configuration as a `.cmx` file. It is recommended that the configuration be backed up in this way before making any changes to the cluster.

**To export the configuration:**

1. From the **File** menu option, select **Export to file**.
2. Select a file name and location. These should be safely recorded for future reference.
3. Click **Save**.

**To import a previously-saved configuration:**

1. From the **File** menu option, select **Import from file**.
2. Confirm.
3. Navigate to the desired configuration (.cmx) file.
4. Click **Open**.

**Unified CVP Media File Upload**

The Cisco Unified Voice Portal (Unified CVP) media file upload provides the capability to provision WAV announcement files directly to the Unified CVP Server. This allows the associated WAV announcement for a Network VRU Script in the Unified ICME/Unified ICMH to be replaced in near real-time. This solution requires your Unified CVP Server(s) to be hosted on Microsoft Windows 2000 Server or
Microsoft Windows Server 2003. Both the web servers hosting Unified CCMP and the Unified CVP Servers must belong to the same domain. This domain may be a Windows 2003 or Windows 2000 domain controller.

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

Below is a brief description of how to set-up the Microsoft Distributed File System and Microsoft File Replication for this application. Both of these technologies are packaged with Microsoft Windows 2000 Server and Microsoft Windows Server 2003.

**Preparing the Configuration**

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

- Make a note of the **Host Name** and **IP Addresses** of ALL of the machines that are hosting Unified CVP.

- Make a note of the **User Name** and **Password** of an administrative user on the domain so that you can configure **File Replication** and the **Distributed File System**.

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

**Configuring DFS for Unified CVP Media File Upload**

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

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

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

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

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

1. Right-click the new root and select the **New Root Target** option from the menu.
2. Enter the **Server Name** for the Unified CVP Server.
3. For the **Folder to Share**, select the folder to contain the Unified CVP media files that are uploaded.
   
   **Note** This folder requires full access security permissions for the Domain Computers group. Configure this for both the shared permissions and the security credentials.
4. Click **Next** to create the Root Target.

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

Configuring File Replication for Unified CVP Media File Upload

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

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

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

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

Performance Configuration Checklists

These checklists are suited to high performance multi-processor machines with 4GB RAM.
### Web Server

<table>
<thead>
<tr>
<th>Done</th>
<th>Description</th>
</tr>
</thead>
</table>
| ☑   | Add the /3GB boot.ini switch to all systems with more than 2GB memory.  
Right-click My Computer and select Properties. The System Properties dialog box is displayed.  
Click the Advanced tab.  
In the Startup and Recovery area, click Settings. The Startup and Recovery dialog box is displayed.  
In the System startup area, click Edit. This opens the Windows boot.ini file in Notepad.  
In the line that states “WINDOWS="Microsoft”, add the following to the end of the line: /fastdetect switch: /3GB.  
Save the changes and close Notepad.  
Click OK twice to close the open dialog boxes. Reboot for the changes to take effect. |
| ☑   | For the IIS DefaultAppPool: disable IIS6 App Pool Shutdown. |
| ☑   | Edit RSReportServer.config: set MaxActiveReqForOneUser = 100.  
RSReportServer.config can be found in C:\Program Files \Microsoft SQL Server\MSSQL \Reporting Services \ReportServer. |
| ☑   | Edit RSReportServer.config: add a key WebServiceUseFileShareStorage = true in the same section as the previous two updates:  
<Add Key="WebServiceUseFileShareStorage" Value="true" /> |

### Database Server

<table>
<thead>
<tr>
<th>Done</th>
<th>Description</th>
</tr>
</thead>
</table>
| ☑   | Add the /3GB boot.ini switch to all systems with more than 2GB memory.  
1. Right-click My Computer and select Properties. The System Properties dialog box is displayed.  
2. Click the Advanced tab. |
3. In the **Startup and Recovery** panel, click **Settings**. The **Startup and Recovery** dialog box is displayed.

4. In the **System startup** panel, click **Edit**. This opens the Windows **boot.ini** file in Notepad.

5. In the line that states “WINDOWS="Microsoft”, add the following to the end of the line: /fastdetect switch: /3GB.

6. Save the changes and close Notepad.

7. Click **OK** twice to close the open dialog boxes. Restart the computer for the change to take effect.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Split ReportServerTempDB into multiple files.</td>
</tr>
</tbody>
</table>
5. Post Installation Steps

Logging in to Unified CCMP

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

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

For 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 not have changed from that previously used.

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

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

Report Uploading

The audit report template must be uploaded into the system. To upload the report into Unified CCMP system:

In your Windows desktop, click Start > All Programs > Management Portal > Report Uploader > Audit Report Uploader.

The Upload Audit Reports dialog window is displayed.

1. Enter administrator in the User Name field.
2. Enter your administrator password in the Password field.
   *Note* You must have specified a new administrator password in the Management Portal, as described above, in order to perform this task.
3. Click Upload.

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

Security Hardening

The Unified CCMP platform may be hardened by using the standard UCC Security Wizard provided with Unified CCE / Unified CCH. This tool may be copied from the Unified ICM (location C:\CiscoUtils) to the same location on the Unified CCMP Servers. Running the UCCSecurityWizard.hta application located in C:\CiscoUtils\UCCSecurityWizard will then allow hardening to be applied.

It is recommended that Security Hardening and Windows Firewall config be performed after the initial installation and configuration of Unified CCMP.
The following ports on the Unified CCMP servers will be configured for access in the Windows Firewall configuration, either by granting the associated executables open access or by opening the specific ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Used by Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Web Application</td>
</tr>
<tr>
<td>443</td>
<td>Web Application when using SSL configuration</td>
</tr>
<tr>
<td>1433</td>
<td>Application Server, Provisioning Server and Data Import Server for database communication.</td>
</tr>
<tr>
<td>2098, 2099, 3333, 3334</td>
<td>Default ports used by the Provisioning Server for ConAPI communication.</td>
</tr>
</tbody>
</table>

It is also recommended that the Cisco Security Agent (CSA) is installed on all machines running Unified CCMP.

Unified CCMP servers may also be configured inline with the following NSA guides for customers with additional security hardening requirements.

Windows Guide (IIS)

.NET 2.0 Hardening Guide

SQL 2005 Hardening Guide
6. Upgrading From a Previous Version

This chapter details how to upgrade from previous Unified CCMP versions to version 8.0(1).

Overview

To upgrade Unified CCMP, it is necessary to uninstall all of the components except for the Database Server component. Because previous versions of the Unified CCMP ran on Microsoft SQL Server 2000, it is necessary to upgrade to Microsoft SQL Server 2005 (either Standard or Enterprise edition). The new version of the Unified CCMP is then installed, and your database upgraded.

Caution Back up all your servers, especially your publisher database server, before you begin.

Uninstalling the Portal

Uninstalling Data Import Server Component

This process will remove the Data Import Server component. This will remove the ability to import data from remote datasources (such as Unified ICME/Unified ICMH or Unified CM) to Unified CCMP datamart.

Removing Replication

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

First, you must stop the Management Portal Data Import service. To do this, proceed as follows:

1. In your Windows desktop, click Start > Run. The Run dialog window is displayed.
2. In the Open field, enter services.msc. The Services dialog window is displayed.
3. Right Click the Management Portal Data Import service from the list of services.
4. Select Stop.
5. Close the Services dialog window.

You may now remove replication.

1. Ensure you are logged in as a domain level user with administrative rights over both database servers.
2. Navigate to the Start > All Programs > Management Portal > Data Import Server and click the Cluster Configuration application.
3. Select the Portal Databases tab.
4. Click Replication.
5. Click **Unreplicate** to remove replication.

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

Once replication has been successfully removed then you may proceed.

**Uninstalling Data Import Server Component**

1. In your Windows desktop, click **Start > Control Panel > Add or Remove Programs**. The **Add/Remove Programs** list is displayed.

2. Select **Management Portal: Data Import Server**.

3. Click **Remove**. A dialog window is displayed asking you if you are sure that you wish to remove the **Management Portal: Data Import Server**.

4. Click **Yes**. The **Setup Status** dialog window is displayed. The extent of the uninstallation progress is displayed on the progress bar.

5. Restart if prompted to do so.

**Uninstalling the Provisioning Server Component**

This process will remove the Provisioning Server component, removing Unified CCMP connection for any remote datasources, such as Unified ICME / Unified ICMH or Unified CM.

In your Windows desktop, click **Start > Control Panel > Add or Remove Programs**. The **Add/Remove Programs** list is displayed.

1. Select **Management Portal: Provisioning Server**.

2. Click **Remove** and confirm.

3. When prompted, click **Yes** to complete uninstallation and restart the system.

4. Manually delete the folder: `C:\Program Files\Management Portal\Provisioning Server\Config`.

**Uninstalling Other Components**

You can uninstall all other components of Unified CCMP by clicking **Remove** from the **Add/Remove Programs** window. Uninstall the components in the following order:

3. Management Portal: Reporting Extensions (Reporting Extensions component)

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


   **Note** This step uninstalls the database setup wizard only. Uninstalling the setup wizard does not affect the database itself. The database itself must not be removed.

Once uninstallation is complete, restart the ReportServer service.
Upgrading Microsoft Microsoft SQL Server

Upgrading to Microsoft SQL Server 2005 Enterprise Edition

Upgrading Microsoft Microsoft SQL Server
Insert your Microsoft SQL Server 2005 Enterprise Edition CD and begin the upgrade process, clicking Next to go through the screens in turn. When prompted to select components, check the boxes for the following:

- Microsoft SQL Server Database Services
- Reporting Services
- Workstation Components

Configuring the NT AUTHORITY\NETWORK SERVICE account

2. From the panel on the right, delete the NT AUTHORITY\NETWORK SERVICE account.
3. In the left-hand navigation panel, click the server name, navigate to Security and click Logins.
4. Double click NT AUTHORITY\NETWORK SERVICE to open its properties.
5. Click User Mappings.
6. Check Portal Database, and select it to see possible roles listed in the box below.
7. In the Database Role Membership For: Portal box, ensure that the following roles are checked:
   - public
   - portalreporting_role
   - portalrs_role
   - db.owner
8. Install Service Pack 3.
You can then proceed to installing the new version of the Management Portal.

Upgrading to Microsoft SQL Server 2005 Standard Edition


Backing Up Databases
Back up the Portal and ReportServer databases so that you can restore them after installing Microsoft SQL Server 2005.

1. Go to Start > All Programs > Microsoft SQL Server > Enterprise Manager.
2. Navigate to the Portal database.
3. Right-click Portal and select Backup. Save the .bak file to a suitable location.
In most cases the .bak file is sufficient to restore the database, but if this fails you will need to restore from the data files.

Back these up as described below:

1. Right-click Portal and select Detach database. This ensures that the data files are in a stable state for copying.
2. Manually copy the data files to a suitable location.

In a similar fashion, back up the ReportServer databases:

1. Run the command services.msc.
2. Stop the ReportServer service.
5. Save the data files to a suitable location.
7. Run services.msc and restart the ReportServer service.

Uninstalling Microsoft SQL Server 2000

1. Go to Start > Control Panel > Add or Remove Programs. The Microsoft SQL Server 2000 programs must be uninstalled in the following order:
   • Microsoft SQL Server2000 ReportServer Enterprise Edition (restart after uninstallation if prompted to do so).
   • Microsoft SQL Server2000 Analysis Services (if present).
   • Microsoft SQL Server2000
2. Restart the computer.

Installing Microsoft SQL Server 2005 Standard Edition

1. Insert the CD for Microsoft SQL Server 2005 Standard Edition and install as normal.
2. Install Service Pack 3.
3. Restart the computer.

Restoring the Databases

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

1. Go to Start > All Programs > Microsoft SQL Server> Management Studio.
2. Click the Restore Database option.
3. Select the backup file (Portal.bak) to restore the Portal database.

   Note If restoring any of the databases fails, it is also possible to restore the database using the .mdf files previously backed up. This procedure is described in its own section, below.

4. Run the services.msc command and stop the Microsoft SQL Server Reporting Services ((MSSQLSERVER) service.
5. Go to Start > All Programs > Microsoft SQL Server> SQL Server Management Studio.

6. Click the Restore Database option.

7. Select the backup files to restore the ReportServer and ReportServerTempDB databases.

8. **Note** The default path for ReportServer data files differs between Microsoft SQL Server 2000 and SQL 2005. To see or change the location to which the databases will be installed, go to the Options page.

It is now necessary to upgrade the ReportServer and ReportServerTempDB databases.

**Restoring the Databases from the Data Files**

If the databases fail to restore from the backup files, it is possible to restore them from the data files.

**For the Portal database:**
1. Copy the Portal data files into an appropriate location.
2. Using Management Studio, click the Attach Database option. You can see and edit the file path for the database from the Options page.
3. Select the Portal.mdf file and reattach.

**For the ReportServer and ReportServerTempDB database:**
1. Ensure the Microsoft SQL Server Reporting Services ({MSSQLSERVER}) service is stopped.
3. Copy the Microsoft SQL Server 2005 ReportServer and ReportServerTempDB data files to a suitable location in case the changes need to be reverted.
   **Note** The default path for ReportServer data files differs between Microsoft SQL Server 2000 and SQL 2005.

7. Run services.msc and restart the ReportServer service.

You can now upgrade the databases.

**Upgrading the Databases**

This step upgrades the ReportServer and ReportServerTempDB databases. The Portal database will be upgraded by the Portal installer in a later step.

1. Open the Reporting Services Configuration Manager and connect to your 2005 instance.
2. Click **Database** Setup and ensure the **Database Name** is **ReportServer**.
3. Click **Upgrade** and confirm.

It will also be necessary to delete the old encryption keys and set up new ones.
1. From the **Reporting Services Configuration Manager** select **Encryption Keys**.
2. Click **Delete** and confirm.
3. Click **Initialization**.
4. Check the box for the first key and click **Remove**.
5. Click **Initialize** and a new key will be created.
6. Restart the computer.

**Configuring the NT AUTHORITY\NETWORK SERVICE account**

1. Using **Management Studio**, navigate to **Databases > Portal > Security** and click **Users**.
2. From the panel on the right, **delete** the **NT AUTHORITY\NETWORK SERVICE** account.
3. In the left-hand navigation panel, click the server name, navigate to **Security** and click **Logins**.
4. Double click **NT AUTHORITY\NETWORK SERVICE** to open its properties.
5. Click **User Mappings**.
6. Check **Portal Database** and select it to see possible roles listed in the **Database Role Membership For: Portal** box below.
7. In the **Database Role Membership For: Portal** box, ensure that the following roles are checked:
   - public
   - portalreporting_role
   - portalrs_role
   - db.owner

You can then proceed to installing the new version of the Management Portal

**Installing the Portal**

Install the new version of the Management Portal as described in Chapter 4 Component Installation. During installation of the Database Component, you must select the option to upgrade an existing database rather than installing a new database.

**Configuration**

Once the database has been upgraded you must configure the system using Configuration Manager as described in Chapter 4 Component Configuration.
7. Platform Uninstallation

This chapter details how to remove Unified CCMP platform components from the platform. The un-installation procedure should be performed in the following order:

Uninstalling Data Import Server Component

This process removes the Data Import Server component. Doing this removes the ability to import data from remote datasources (such as Unified ICME/Unified ICMH or Unified CM) to Unified CCMP datamart.

Removing Replication

If you have a dual-sided installation, follow these steps to remove replication. First, you must stop the Management Portal Data Import service. To do this, proceed as follows:

1. In your Windows desktop, click Start > Run. The Run dialog window is displayed.
2. In the Open field, enter services.msc. The Services dialog window is displayed.
3. Right click the Management Portal Data Import service from the list of services.
4. Select Stop.
5. Close the Services dialog window.
   You may now remove replication.
6. Ensure you are logged in as a domain level user with administrative rights over both database servers.
7. Navigate to the Start > All Programs > Management Portal > Data Import Server and click the Cluster Configuration application.
8. Select the Portal Databases tab.
9. Click the Replication button.
10. Click the Unreplicate button to remove replication.
    Note Removing replication may take some time.

Once replication has been successfully removed, you may proceed.

Uninstalling Data Import Server Component

1. Insert the CD that came with your old version of the Unified CCMP. Close any windows that automatically open.
2. In your Windows desktop, click Start > Control Panel > Add or Remove Programs. The Add/Remove Programs list is displayed.
4. Click the Remove option. A dialog window is displayed asking you if you are sure that you wish to remove the Management Portal: Data Import Server.
5. Click Yes. The Setup Status dialog window is displayed. The extent of the uninstallation progress is displayed on the progress bar.

Uninstalling the Database Component

This process removes the database installation component and Unified CCMP database catalogs. Do not remove the database catalogs from your system unless you intend to permanently remove Unified CCMP, or unless you have been instructed to do so by support personnel.

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

1. From your Management Portal CD, run the file autorun.bat.
2. Select the Database Server component, click Run Test.. and, when that has completed, Install.
3. Continue through the installation process, agreeing with the license agreement and accepting the defaults if necessary, until you reach the Select an Action to perform screen.
4. Select Delete an existing database and click Next.
5. Unless working with a customized installation of Microsoft SQL Server, ignore the fields on the Configure the Location of Data Files screen and click Next.
6. In your Windows desktop, click Start > Control Panel > Add or Remove Programs. The Add/Remove Programs list is displayed.
8. Click the Remove option, and confirm.

Uninstalling All Other Components

All other components can be uninstalled by simply clicking Remove from the Add/Remove Programs window. Uninstall them in the following order:


Note In some circumstances, uninstallation may not be able to stop Microsoft Reporting Services in a timely fashion. If an error occurs during uninstallation, use the services.msc command to check that the ReportServer service is stopped. Then re-attempt uninstallation. Once uninstallation is complete, restart the ReportServer service.
8. Glossary

A

Audit
A diagnostic process instigated to assess system performance.

C

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

Certificate Authority
A certificate authority (CA) issues and manages security credentials and public keys for message encryption across a network. The CA checks with a Registration Authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.

Certificate Revocation Lists (CRL)
A method for maintaining access to network servers. The CRL is a list of subscribers paired with digital certificate status. The list describes revoked certificates along with the reason(s) for revocation. The dates of certificate issue and the entities that issued them are also included. Additionally, each list contains a proposed date for the next release. When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user.

Cipher
A method used to encrypt text.

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

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

Configuration
The hardware and/or software components that comprise a system and the manner in which they are connected.
Connection
The link between two nodes in a script or between a node and a routing target set. Connections show the flow of control between objects in the script. Within the Script Editor, a connection is represented as a line segment.

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

Cookie
Information sent by a web server to a web browser when the browser first visits a web site. The information is stored in a text file that is sent to that web server each time the browser requests information from it.

Comma Separated File (.CSV)
A method of representing a spreadsheet using a text file. The values are separated by commas, and each record is ended by a line break. The column headers are contained in the first record

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

Dynamic Link Library (DLL)
A list of executable functions or data that can be used by a Windows application. The DLL provides the functions, and a program accesses them by creating either a static or a dynamic link to the DLL. A static link remains constant while the program is being executed, while a dynamic link is created by the program when it is needed.

Event Log
A software tool that records and displays user actions or system events.

Failover
A back up process used when the primary process fails.

Field
A space in a database allocated to an item of information. A collection of fields is called a record.
Firewall
A security measure placed between trusted and un-trusted sites. It filters out traffic that can damage the host network or connected hardware.

Flag
A means of highlighting a particular condition or status in a hardware or software system. A flag can either be set to on or off.

Graphical User Interface (GUI)
A point-and-click interface within Windows applications allowing the user to interact with a software program without the need to write code.

Hash
Unified CCMP uses hashed values for security purposes. A hash value or message digest is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is highly likely to be a unique value. Hashed values are used to ensure that transmitted messages have not been tampered with. The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they are identical, there is a high probability that the message was transmitted intact.

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

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

Logger
A software application that logs events.

Map
A map is used to logically connect two entities. As programs cannot translate directly from human concepts to computer numbers, the concepts are translated incrementally through a series of layers. Each layer contains the same amount of information as the layer above but in a closer form to that which the computer understands. This process of translating from one layer to another is called mapping.
**Metadata**
Data about data. Metadata describes how, when, and by whom particular data has been collected and how the data is formatted.

**Polling**
The Provisioning component sends a regular ping to the IVR to ensure it is still online and functioning according to scripted parameters.

**Remote Transfer**
A protocol used by the Provisioning component to transfer customer script to a remote Provisioning component.

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

**Secure Sockets Layer (SSL) – (See HTTPS)**

**Simple Network Management Protocol (SNMP)**
A protocol designed to enable the remote management of a computer network by polling and setting terminal values and monitoring network events. SNMP enables communication between different types of network and allows different types and brands of network peripherals (hubs, bridges, routers, and so forth) to be managed by a single piece of network management software.

**Structured Query Language (SQL)**
A database query language in which statements are formulated to manipulate or request data in a database.

**Microsoft SQL Server**
The Microsoft relational database product used for the Unified ICME/Unified ICM local and central databases

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

**Synchronous**
Occurring at regular intervals. The opposite of synchronous is asynchronous. Communication within a computer is usually synchronous and is governed by the microprocessor clock; for example, signals along the bus can occur only at specific points in the clock cycle.
Thread
A part of a program that can be executed independently of other parts.

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

Web Browser
A software application used to locate and display Web pages.

Wide Area Network (WAN)
The connection of several computers across a wide area, normally using telephone lines.

World Wide Web (WWW)
A system of Internet servers that support documents formatted in HTML. The World Wide Web supports links to other documents, as well as graphics, audio and video files. This means you can jump from one document to another simply by clicking on a link.
## 9. Index

<table>
<thead>
<tr>
<th>A</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Instance List</td>
<td>Encrypt</td>
</tr>
<tr>
<td>Audit</td>
<td>Encryption keys</td>
</tr>
<tr>
<td>B</td>
<td>F</td>
</tr>
<tr>
<td>Back up</td>
<td>FTP</td>
</tr>
<tr>
<td>BITS</td>
<td>I</td>
</tr>
<tr>
<td>C</td>
<td>ICM</td>
</tr>
<tr>
<td>CallManager</td>
<td>IPCC</td>
</tr>
<tr>
<td>CICM</td>
<td>L</td>
</tr>
<tr>
<td>9, 35</td>
<td>Load balancing</td>
</tr>
<tr>
<td>Cisco Security Agent (CSA)</td>
<td>M</td>
</tr>
<tr>
<td>17</td>
<td>Microsoft Distributed File System</td>
</tr>
<tr>
<td>Cluster</td>
<td>Microsoft Terminal Services</td>
</tr>
<tr>
<td>CMS Server</td>
<td>N</td>
</tr>
<tr>
<td>29</td>
<td>NAM</td>
</tr>
<tr>
<td>Commissioning</td>
<td>NT AUTHORITY\NETWORK SERVICE</td>
</tr>
<tr>
<td>Component</td>
<td>P</td>
</tr>
<tr>
<td>11</td>
<td>Performance Configuration Checklists</td>
</tr>
<tr>
<td>ConAPI</td>
<td>Prerequisite Software</td>
</tr>
<tr>
<td>Connections</td>
<td>Provisioning</td>
</tr>
<tr>
<td>CVP Media File Upload</td>
<td>Publisher</td>
</tr>
<tr>
<td>CVP tools</td>
<td>R</td>
</tr>
<tr>
<td>9</td>
<td>Reboot</td>
</tr>
<tr>
<td>D</td>
<td>Report Uploading</td>
</tr>
<tr>
<td>Data replication</td>
<td>Resilience</td>
</tr>
<tr>
<td>Database</td>
<td>Secure Deployment</td>
</tr>
<tr>
<td>Backup</td>
<td>Security Hardening</td>
</tr>
<tr>
<td>Replication</td>
<td>SNMP traps</td>
</tr>
<tr>
<td>Restore</td>
<td>SQL Server Agent service</td>
</tr>
<tr>
<td>Decrypt</td>
<td>sql_agent_user</td>
</tr>
<tr>
<td>Dedicated Server</td>
<td>10</td>
</tr>
<tr>
<td>Demilitarized zone (DMZ)</td>
<td>10</td>
</tr>
<tr>
<td>Deployment</td>
<td>10</td>
</tr>
<tr>
<td>Models</td>
<td>Secure Deployment</td>
</tr>
<tr>
<td>Specifics</td>
<td>Security Hardening</td>
</tr>
<tr>
<td>Distributor</td>
<td>SNMP traps</td>
</tr>
<tr>
<td>Domain controller</td>
<td>SQL Server Agent service</td>
</tr>
<tr>
<td>Dual-sided</td>
<td>sql_agent_user</td>
</tr>
<tr>
<td>Subscriber</td>
<td>User interface</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>27</td>
<td>8</td>
</tr>
<tr>
<td>Transaction log</td>
<td>VRU</td>
</tr>
<tr>
<td>14</td>
<td>39</td>
</tr>
<tr>
<td>Uninstallation</td>
<td>WAV</td>
</tr>
<tr>
<td>53</td>
<td>39</td>
</tr>
<tr>
<td>Upgrade</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td></td>
</tr>
</tbody>
</table>