Installation and Configuration Guide for Cisco Unified Contact Center Domain Manager

Release 9.0(1)

August 2012

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

Purpose

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

Audience

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

Organization

The sections of this guide are as follows:

Chapter 1	Planning Your Installation	Introduces Unified CCDM, including its integration with Unified CCE.
Chapter 2	Installation Guidelines and Requirements	Lists the prerequisites for Unified CCDM installation and provides recommendations for pre installation platform configuration.
Chapter 3	Windows and SQL Component Installation	Describes how to setup the Microsoft SQL Server.
Chapter 4	CCDM Component Installation	Provides instructions for the installation of all Unified CCDM components.
Chapter 5	Unified CCDM Component Configuration	Describes post-installation configuration of Unified CCDM, including setting up replication and uploading .wav files for voice announcements. The procedure for configuring a Unified CCDM server cluster is detailed as well as how to use the Unified CCDM Replication Manager to replicate data

		between Database servers. Web and Database component server performance checklists are also provided.
Chapter 6	Post Installation Steps	Describes the post-installation options and the system checks for the Unified CCDM platform.
Chapter 7	Uninstalling Unified CCDM	Describes how to remove Unified CCDM platform from your servers.
Chapter 8	Troubleshooting	Describes how to enable logging for the Unified CCDM Installer and how to apply database permissions after the Installer has completed.

Related Documentation

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

- Related documentation includes the documentation sets for Cisco CTI Object Server (CTIOS), Cisco Agent Desktop (CAD), Cisco Agent Desktop - Browser Edition (CAD-BE), Cisco Unified Customer Voice Portal (CVP),Cisco Unified IP IVR, Cisco Unified Intelligence Center, and Cisco Support Tools.
- For documentation for these Cisco Unified Contact Center products, go to http://www.cisco.com/cisco/web/psa/default.html, click **Voice and Unified Communications**, then click **Customer Contact**, then click **Cisco Unified Contact Center Products** or **Cisco Unified Voice Self-Service Products**, then click the product/option you are interested in.
- For troubleshooting tips for these Cisco Unified Contact Center products, go to http://docwiki.cisco.com/wiki/Category:Troubleshooting, then click the product/option you are interested in.
- Documentation for Cisco Unified Communications Manager is accessible from: http://www.cisco.com/cisco/web/psa/default.html.
- Technical Support documentation and tools are accessible from: http://www.cisco.com/en/US/support/index.html.
- The Product Alert tool is accessible from (sign in required): http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice.
- For information on the Cisco software support methodology, refer to *Software Release and Support Methodology: ICM/IPCC* available at (sign in required): http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/prod_bulletins_list.html.

For a detailed list of language localizations, refer to the *Cisco Unified ICM/Contact Center Product and System Localization Matrix* available at the bottom of the following page:

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html.

Product Naming Conventions

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

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

Old Product Name	New Name (long version)	New Name (short version)
Cisco IPCC Enterprise Edition	Cisco Unified Contact Center Enterprise	Unified CCE
Cisco IPCC Hosted Edition	Cisco Unified Contact Center Hosted	Unified CCH
Cisco Intelligent Contact Management (ICM) Enterprise Edition	Cisco Unified Intelligent Contact Management (ICM) Enterprise	Unified ICM
Cisco Intelligent Contact Management (ICM) Hosted Edition	Cisco Unified Intelligent Contact Management (ICM) Hosted	
Cisco CallManager/Cisco Unified CallManager	Cisco Unified Communications Manager	Unified CM

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as entries, keys, buttons, folders and submenu names. For example: • Choose **Edit** > **Find** • Click **Finish**
italic font	Italic font is used to indicate the following: • To introduce a new term; for example: A skill group is a collection of agents who share similar skills

	• For emphasis; for example: Do not use the numerical naming convention • A syntax value that the user must replace; for example: IF (condition, true-value, false-value) • A book title; for example: Refer to the Cisco CRS Installation Guide
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays; for example: `<html><title>Cisco Systems, Inc. </title></html>`
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output • A character string that the user enters but that does not appear on the window, such as a password

Obtaining Documentation and Submitting a Service Request

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

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

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

Documentation Feedback

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

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.

1. Planning Your Installation

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

Deployment Specifics

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

Each configured Unified CCE instance must have its own:

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

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

System Architecture

Infrastructure Software

Windows 2008 Server R2 with Service Pack 1.

SQL Server 2008 R2 Standard Edition with Service Pack 1.

Deployment Models

In many environments, Unified CCDM is installed using a dual-sided deployment model to provide load balancing, resiliency, and high availability. For deployments that require layered security, such as Internet-facing environments, both sides are

split across separate database servers and web/application servers are separated by a demilitarized zone (DMZ).

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

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

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

Unified CCDM Architecture

A Unified CCDM installation comprises the following components.

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

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

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

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

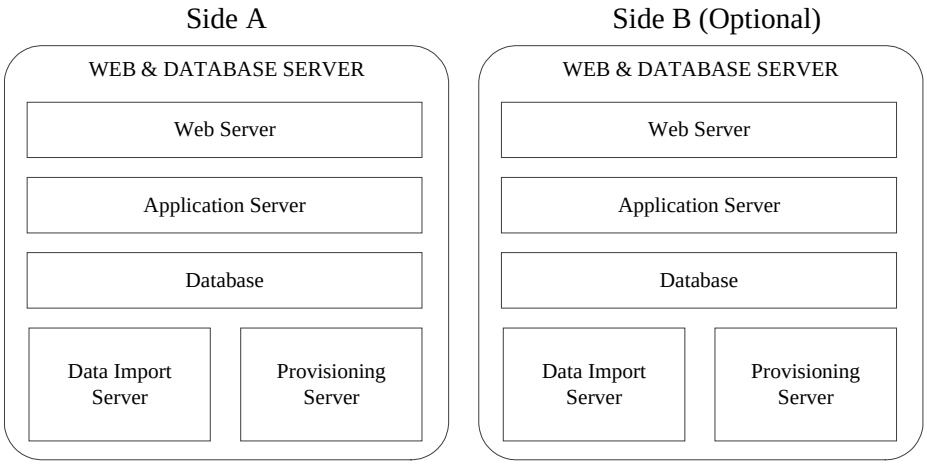
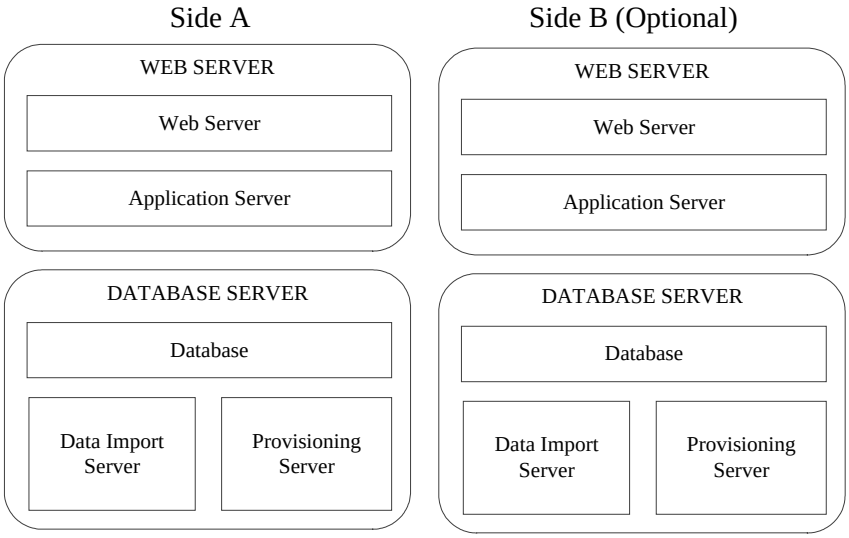


Figure 2, below, describes the software installation layout for a dual tier deployment. The web server and application server components reside on a separate server. Optionally, a second side can be included for resilience.

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



2. Installation Guidelines and Requirements

Installation Prerequisite Checklist

Each CCDM component requires prerequisite software and Windows features to be installed in order to operate correctly.

A mandatory check is performed before each part of the installation that checks the required pre-requisite software elements. If this check does not find the required software then the installation will not proceed.

Windows Feature Requirements

The following Windows 2008 R2 features are required on all Servers hosting CCDM:

- Microsoft .NET Framework 3.5 SP1
- TCP Activation
- Named Pipes Activation
- File Server

In addition to these features the following components must also be enabled on the associated servers:

- Machines hosting the Database Server component
  - Incoming Remote Transactions
  - Outgoing Remote Transactions
- Machines hosting the App/Web Server Component
  - IIS Elements
    - Static Content
    - Default Document
    - Directory Browsing
    - HTTP Errors
    - ASP.NET

    - .NET Extensibility
    - ISAPI Extensions
    - ISAPI Filters
    - HTTP Logging
    - Request Monitor
    - Basic Authentication
    - Windows Authentication
    - Request Filtering
    - Static Content Compression
    - IIS Management Console
    - IIS 6 Management Compatibility
  - Web Server (IIS) Tools

Windows feature requirements for each component are tested by the CCDM deployment utility contained on the DVD. Should the required features be missing then they may be configured by clicking on the **Windows features enabled** option from within the deployment tool.

A summary of the software prerequisites for CCDM is as follows. Some prerequisites software is distributed with CCDM and will be installed automatically if it is missing from the server.

Note

Pre-requisite software that is not distributed with CCDM is marked in **bold** in the list below and must be installed on the appropriate servers before the CCDM installation is performed.

Database Server Component

- **Windows Server 2008 R2 SP1**
- **Microsoft SQL Server 2008 R2 SP1 64-bit Standard Edition**
- **Microsoft SQL Server 2008 R2 Workstation Components**
- J2SE Runtime Environment 6.0 (Update 30)

App/Web Server Component

- **Windows Server 2008 R2 SP1**
- ASP .NET State Service Enabled

General Guidelines

- Do not install any CCDM component on a domain controller.
- Install Internet Explorer (IE) 7 or later on all the machines from which CCDM will be accessed.

Server Requirements

- CCDM servers should be configured to use the US English character set.
- CCDM server names must consist of alphanumeric characters only, without underscores or hyphens.
- Configure Microsoft Terminal Services for remote configuration and support.
- In the Event Viewer, set the Application Log, Security Log and System Log to **Overwrite events as needed**.

Network and Environment Configuration

This section describes the network interaction performed by the various components of Unified CCDM. Its content can be used by network administrators to configure network requirements to ensure that CCDM obtains the required access levels for each component.

IPV6 Support

CCDM runs on systems equipped with IPv6 hardware, but requires that all CCDM Servers have an IPv4 address and IPv6 disabled on the NIC used by CCDM.

Firewalls

In many CCDM configurations, Firewalls will be deployed both between the CCDM servers (to create a DMZ) and possibly between CCDM DB servers and the Unified CCE AWs. Care must be taken in these configurations to ensure that the correct firewall ports are opened to both-way traffic.

The Windows 2008 R2 platform incorporates its own software based firewall that must be configured to allow the various components of Unified CCDM to communicate with one another in a distributed environment.

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

Note These tables do not include standard Windows ports such as DNS and Kerberos. Ports are also required to access all CCDM servers for support purposes (either Terminal Services or Remote Desktop).

Web Server Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Used by	Usage
HTTP	TCP	80	End User	Web application
HTTPS	TCP	443	End User	Web application
Web Service Subscriptions	TCP	8083	Customer Applications	Customer Specific
Web Service Notifications	TCP	8084	Customer Applications	Customer Specific
Web Service Resource Management	TCP	8085	Customer Applications	Customer Specific

CCDM Database Server Port Usage

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

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

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

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

Cisco Unified CCE Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Used by	Usage
SQL Server	TCP	1433	Data Import Services, Provisioning Services, Application Services	Importing Dimension Data, Provisioning Activities, Real-time Reports.
ConAPI Remote Registry	TCP	2099*	Provisioning Services	Provisioning
CMS Node	UDP	9000	Provisioning Services	Ping Port for ConAPI services

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

Domain Controllers for Unified CCE Instances Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Used by	Usage
LDAP	TCP	389	Application Services	Supervisor domain account provisioning

Cisco Unified CM Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Used by	Usage
AXL Web Service (HTTPS)	TCP	443	Provisioning Services, Data Import Services	Importing and Provisioning

Other Information

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

- Distributed Transaction Coordinator

- File and Printer Sharing.

3. Windows and SQL Component Installation

Windows – All Servers

Ensure that FIPS compliance checking is turned off. To do this:

1. Click **Start > All Programs > Administrative Tools > Local Security Policy** from the start menu.
2. Open **Local Policies** folder and click **Security Options** to see the list of policies.
3. Ensure the policy **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** is disabled.
4. Close the window.

User Account Control (UAC) is a Windows feature that was introduced to protect the operating system from malicious programs. UAC must be disabled on all servers before CCDM installation begins. If UAC is enabled it may cause issues with the software used to install CCDM. To disable UAC perform the following steps:

1. Click **Start** > **Control Panel > User Accounts > User Accounts > Change User Account Control settings**.
2. Use slide bar to select **Never Notify** option to disable UAC.
3. Click **OK**.
4. Restart your machine to commit the new UAC settings.

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

SQL Server

Follow these installation instructions to install SQL Server on the server(s) that will be hosting the Unified CCDM Database:

1. When presented with the SQL Server Installation Center select the **Installation** menu option from the left of the window.
2. Select **New installation or add features to an existing installation**.

3. The Setup Support Rules window will display validating the system for the installation of SQL Server 2008 R2. Once validation passes click the **OK** button to proceed.
4. Enter the product key for SQL Server 2008 R2 and click **Next**.
5. Read the license terms for SQL Server 2008 R2, if you agree with the terms check the **I accept the license terms** checkbox and click **Next**.
6. You will be prompted to install the Setup Support Files. Click **Install**.
7. Once the Setup of Support Files is complete you will be presented with a summary of checks. Review the results and make any necessary changes. If you see a warning saying that Windows Firewall is enabled, you can safely ignore it. When you are satisfied, click **Next** to proceed.
8. Select the **SQL Server Feature Installation** option and click **Next**.
9. Select the following Instance Features:
   - **Database Engine Services**
     - **SQL Server Replication**
   - **Client Tools Connectivity**
   - **Management Tools – Basic**
     - **Management Tools – Complete**
10. Update the installation directories to install in the required locations. Click **Next**.
11. Installation Rules will then be checked. Correct any issues that have been flagged by the Installation Rules check and then click **Next** to proceed.
12. The Instance Configuration window is displayed. Select **Default Instanc**e, with an Instance ID of **MSSQLSERVER**. Update the Instance root directory to be installed on the required drive, click **Next** to proceed.
13. The Disk Space Requirements summary window is displayed, click **Next**.
14. In the Server Configuration window, on the **Service Accounts** tab, set the following service configuration:
    - Locate the SQL Server Agent entry in the Service column, and set the corresponding Account Name to **NT AUTHORITY\SYSTEM** and the Startup Type to **Automatic**.
    - Locate the SQL Server Database Engine entry in the Service column and set the corresponding Account Name to **NT AUTHORITY\SYSTEM**.
15. In the Server Configuration window, on the **Collation** tab, ensure that the Database Engine is configured with **Latin1_General_CI_AS** (Latin1_General, Case In-sensitive, Accent Sensitive) collation. Click **Next** to proceed.
16. The Database Engine Configuration window is displayed.

- Select **Mixed Mode** authentication and enter a password for the sa user.
- In the Specify SQL Server administrators panel click the **Add Current User** button. Also add any other accounts that require administrator permissions to the Database, for example, Domain Admins, Service Accounts etc.
- Click **Next** to proceed.

17. The Error Reporting window is displayed. Click **Next** to proceed.
18. The Installation Configuration Rules window is displayed and installation checks are performed. Correct any reported problems and click **Next** to proceed.
19. Review the installation summary and click **Install** to begin installing SQL Server 2008 R2.
20. Once the installation is complete click the **Close** button. Installation of SQL Server 2008 R2 is complete.

Note

When the SQL Server 2008 R2 installation is complete, locate and install SQL Server 2008 R2 Service Pack 1 before proceeding.

Post-Installation Configuration

SQL Server – Database Server

Configure Distributed Transaction Coordinator (DTC)

Configure Distributed Transaction Coordinator (DTC) as follows:

1. Click **Start** > **All Programs** > **Administrative Tools** > **Component Services**. The Component Services management tool is displayed.
2. Expand **Component Services** > **Computers** > **My Computer** > **Distributed Transaction Coordinator**.
3. Right-click on **Local DTC** and select **Properties**. The Local DTC Properties window is displayed.
4. Select **Security** tab.
   - Ensure that **Security Settings** has **Network DTC Access** selected, and that **Transaction Manager Communication** has **Allow Inbound** and **Allow Outbound** selected.
   - Set **Transaction Manager Communication** to **No Authentication Required**.
   - Click **OK** and accept the prompt to restart the MSDTC Service.
5. Close the Component Services window.

Configure SQL Server Network Protocols

To configure SQL Server network protocols follow these steps:

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

Configure Windows Server 2008 R2 Firewall for SQL Server

By default the Windows Server 2008 R2 Firewall will not allow incoming traffic for SQL Server. If the Windows firewall is enabled, follow these steps to create a rule to allow SQL Server traffic:

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

SQL Server Backup Guidelines

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

Required User Accounts

CCDM Service Accounts

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

Accounts for Replication

You will need to create the following domain user account for CCDM. Using Active Directory, create this account with the following attributes:

- Password never expires
- User cannot change password

sql_agent_user

A domain account is used by SQL Server to replicate data between SQL Server databases. By default CCDM assumes this will be `sql_agent_user`, but a different account name may be specified during installation.

4. CCDM Component Installation

Planning Your Installation

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

Recording Your Settings

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

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

The Unified CCDM Installer

Start the Unified CCDM Installer

1. Insert the Unified CCDM DVD. If auto-run is enabled on the server, a window opens automatically showing a list of Unified CCDM components under the heading 'Server Installation' on the left hand side.

Note: If auto-run is disabled and you do not see the Installation Components screen, double-click the **autorun.bat** file located on the DVD to launch the Unified CCDM installer manually.

Note: If UAC has not been disabled, launch the installation manually by right-clicking on the **autorun.ba**t file located on the DVD and selecting **run as administrator** option.

Note: Some anti-virus software may state that the **autorun.hta** script file is malicious. Please ignore and continue with the installation.

2. Follow the steps in the sections below to install each component, but read the information about prerequisites in the rest of this section first.

Before you can install a Unified CCDM component, the prerequisites for that component must be present. The Unified CCDM Installer checks the prerequisites for each component as follows:

- When you click on a component to install it, the installer displays a list of prerequisites for that component and checks that each prerequisite is present. As each prerequisite check completes, you will see a green tick (check successful) or a red cross (check failed). The Install option for that component is only available when all prerequisite checks are successful.
- Where possible, the Unified CCDM DVD includes redistributable packages for prerequisites, so if a prerequisite check fails, you can click on the link in the Unified CCDM installer to install the missing prerequisite. Once all the prerequisite software is installed, you can click on the component again, then click **Rerun** to rerun the tests.
- When all the prerequisites display a green tick, you will be able to click **Install** to install the chosen component.

Unified CCDM Database Server Installation

This section details how to install the Unified CCDM Database Server component.

Install the Database Installer

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

On the Side A Database Server:

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

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

5. In the Configure Database window:
   - **Catalog Name** Enter a name for the database catalog that will be used for Unified CCDM. It is recommended that you use the default name of Portal.
   - **Connect Using** Select the login credentials you want to use:
     - **Windows authentication credentials of application** This is the recommended option
     - **The SQL Server authentication using the login and password below.** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your SQL Server Login ID and Password in the fields provided.
6. In the Destination Folder window, you can click **Change** to change the location for the installation of the Database Server. It is not necessary to install all Unified CCDM components in the same location.
7. In the Setup Type window, select from:

- **Complete** – a complete installation of all of the components. This is the preferred option for most installations.
- **Custom** – allows the user to select from a variety of options that may be installed to the system. This should only be used by advanced users that know explicitly which components need to be installed to the system.

8. In the Session File Folder window you can choose a location for the importer session files. These are temporary files used by the installer.
9. Click **Install.**

Note

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

10. When the installation has completed, if you want to set up your database now, check the **Launch Database Management Utility** check box. You can also set up your database manually at a later date.
11. Click **Finish**.

Database Setup

If you selected the Launch Database Management Utility check box after installing the Database component, the database setup wizard will launch automatically. Otherwise you can launch the database install tool manually from **Start > All Programs > Domain Manager > Database > Database Installer**.

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

1. Click **Next** to go through each window in turn. You will need to enter the following details:
2. In the Select an Action to Perform window:
   - **Install a new database** You can maintain this database at a later date by running the installer again and selecting the appropriate option.
3. In the SQL Server Connection Details window:
   - **Server Name** Enter the name of the machine that is to be the Database Server. This should normally be left as the default (local).
   - **Database Name** Enter or select the name of the database catalog that will be used for Unified CCDM. It is recommended that you use the default name of Portal. This should match the database catalog name specified when you installed the database installer. If not, you will see a warning message.
   - **Connect Using.** Select the login credentials you want to use:

- **The Windows account information I use to logon to my computer.** This is the recommended option.
- **The SQL Server login information assigned by the system administrator.** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your SQL Server Login Name and Password in the fields provided.

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

4. In the Setup Replication window, if this database installation is not side B of a replicated system, just click **Next**. If this database installation is side B of a replicated system, select **Replicated Configuration** and set up the replication folder share as follows:
   - **Share Name** The name of the share for the ReplData folder. By default this is ReplData.
   - **Folder Path** The path of the ReplData folder. This is configured in SQL Server, and is by default **C:\Program Files\Microsoft SQL Server\MSSQL\repldata.**
   - Click **Next** when you have finished.
5. In the Configure the Location of Data Files window, if you are not using a custom installation of SQL Server, accept the defaults and click **Next**. If you are using a custom installation of SQL Server, configure the data files as follows:
   - Select the check box or boxes beside the file group or file groups you want to change.
   - To change the **Location**, browse to the new location.
   - To change the **Max Size**, specify the amount of space that should be allocated for the chosen file group or file groups. The default value is based on Unified CCDM's analysis of your system.
   - To specify a different **Initial Size**, first uncheck **Set Initial Size to Max Size**,
   - You can also choose an unlimited file size by selecting **Unrestricted Size**, but this is not recommended.
   - Click **Update** to save your changes to the selected file group or file groups.
   - Click **Default** (in the top right corner of the window) to restore the settings for all file groups to their default.
   - Click **Next** when you have finished.
6. The **Configure SQL Server Agent Service Identity** window sets up a user account that is used by SQL Server for replication:

- **Account Type** The type of user account that will be used. For a distributed installation, this must be Domain.
- **User Name** The name of the user account. This defaults to **sql_agent_user**. If you used a different name when setting up the account, enter that name instead. If you have specified a domain user, you will need to prefix the user name with the domain name, followed by a backslash.
- **Automatically create the user account if missing** If you have not already created the user account on the domain, set it up now as described in section Accounts for Replication on page 14 before continuing. For a single sided single server system, it is possible to create a local user automatically by selecting this check box. Use of a local user will mean system re-installation when adding a second side in the future.
- **Password** Create a password for the new user, conforming to your individual system's complexity requirements.
- **Confirm Password** You will not be able to continue until the contents of this field are identical to the password entered above.
- Click **Next**.

7. In the **Web Application Servers Network Service Configuration** window, enter the details of each remote App/Web Server to be used in the installation. This information only needs to be entered in Unified CCDM deployment models where the web application servers are on a different machine from the database server itself.
   - **Domain** The network domain the web server is on, for example ACMEDOM
   - **Machine Name** The name of the machine, for example WEBSERVERA
   - Click **Add** to add each Web Server to the list.
   - When all Web Servers have been added, click **Next**.
8. In the **Ready to install the Database** window, click **Next** to begin installation. Installation will take several minutes.
9. Click **Close** to close the installer.

Database Replication

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

See section Configuring Replication in Chapter 5 for information about configuring database replication.

App/Web Server Component

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

This section details how to install and configure the Unified CCDM App/Web component.

App/Web Installation

1. To install the Unified CCDM App/Web component, in the Unified CCDM Installer, select **App/Web Serve**r, and wait until the prerequisite checks have completed. If any checks fail, fix them as described above. When all checks have passed, click **Install** to begin the App/Web Server Installation. The **Domain Manager: Application Server Component** window displays.
2. Click **Next** to go through each window in turn. You will need to enter the following details:
3. In the **License Agreement** window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.
4. In the **Cryptography Configuration** window:
   - **Passphrase** Create a cryptographic 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 will not be able to continue until the contents of this field are identical to the passphrase entered above.
   - Click **Next** to continue.

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

5. In the **Destination Folder** window, you can click **Change** to change the location that the App/Web Server components are installed to. Click **Next** to continue.
6. In the **Configure Database** window:
   - **SQLServer Name** Enter the name of the machine that is to be the Database Server. The default of **localhost** is valid only when installing on the Database Server. Otherwise, specify the name of the machine where you installed the database above.

- **Catalog Name** Enter or select the name you selected while installing the Database Server component. By default this is Portal.
- **Connect Using** Select the login credentials you want to use:
  - **Windows authentication** This is the recommended option.
  - **The 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 SQL Server Login Name and Password in the fields provided.
- Click **Next** to continue.

7. Click **Install**.
8. When the installation has completed, click **Finish**.

Note

The machine will restart once the installation is complete.

Support Tools

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

1. To install the Diagnostic Framework component, start the Unified CCDM Installer, click **Support Tools** and select **Diagnostic Framework**. The **Domain Manager: Diagnostic Framework InstallShield Wizard** window displays.
2. Click **Next** to go through each window in turn. You will need to enter the following details:
3. In the **License Agreement** window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.
   - Click **Next**.
4. In the Destination Drive window click **Update** to change the default drive where the Diagnostic Framework will be installed. Click **Next** when you have finished.
5. In the **Select Certificate** window, select the type of certificate installed with the Diagnostic Framework.
   - **Self-Signed Certificate –** A new certificate will be generated by the installer. This type of certificate should be used only for lab or test deployments.

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

6. Click **Install.**
7. When the installation is completed, click **Finish.**

The installation of the Diagnostic Framework component is now complete.

5. Unified CCDM Component Configuration

Unified CCDM will normally be hosted on multiple servers for performance and data security. This chapter describes how to configure the server cluster and perform data replication. It also provides performance tuning checklists for the Web and Database components.

This section describes the following steps:

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

Configuring Unified CCE Admin Workstations

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

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

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

- **General** page:
  - **Login Name**, enter the machine name in the form <DOMAIN>\<MACHINENAME>$, for example ACMEDOM\ACMEWEBA$. This configures access for the NETWORK SERVICE account from the Unified CCDM servers
  - **Authentication**, select Windows Authentication unless connecting to a server on a different domain
- **User Mapping** page:
  - **Users mapped to this login**. select the checkbox for the AWDB database
  - **Database role membership for**. AWDB, check the **Public** and **db_datareader** checkboxes.

6. Click **OK**.

Configuring Unified CCE Admin Workstations for Provisioning

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

Configuration Overview

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

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

An Application Instance must be configured on each AW for Unified CCDM to connect to. If support for provisioning multimedia resources is required, the Application Instance must be configured to **Application Type: <Other>** instead of the standard Cisco Voice.

Multiple Unified CCE instances can be supported, but each requires a distinct primary Distributor AW to connect to:

- ConAPI only supports connection to one Application Instance on each physical server. You must therefore have a separate physical AW distributor for each instance.
- Parent/Child AW configurations are Supported as multiple instances in Unified CCDM.

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

Before beginning cluster configuration, you must set up the ConAPI application instance and the CMS server on the CICM/Unified CCE(s).

Note

This is only necessary on deployments that include resource management.

Common ConAPI Credentials

To create an application instance, you must run Configuration Manager on the Unified CCE AW as follows:

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

Note

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

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

CMS Server Setup

Before configuring the Unified CCDM server cluster you must ensure that the CMS Server(s) are set up correctly on each Unified CCE.

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

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

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

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

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

   - **Application host name** The server name, such as `Unified CCDM`.
3. Click **OK**, and **OK** again to cycle the CMSJServer, save your changes and close the CMS control console.

Configuring the Unified CCDM Cluster

Before Unified CCDM will operate correctly, communications channels between the different Unified CCDM components must be established so that each individual Unified CCDM component knows where to connect and where to establish a connection in the event of a failure.

The ICE Cluster Configuration Tool

The communications channels for the Unified CCDM components are configured using the Cluster Configuration tool in the Unified CCDM Integrated Configuration

Environment (ICE). The Cluster Configuration tool allows configuration of Unified CCDM server clusters, consisting of the Unified CCDM servers, Unified CCEs and Unified CMs.

To start ICE, on the A Side database server:

1. Go to **Start** > **All Programs** > **Domain Manager** > **Configuration Tools** > **Integrated Configuration Environment**.
2. The **Database Connection** window is displayed. In this window specify the following:
   - **Server Name** This option defaults to the current machine.
   - **Database Name** Select the Unified CCDM database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
   - **Authentication** Ensure this option is set to Windows Authentication.
3. Click **OK** to open ICE. When ICE starts, the Cluster Configuration tool is loaded as the default tool. You can use the Tool drop-down in the toolbar to switch to other ICE tools.

The rest of this section describes how to use the ICE Cluster Configuration tool to configure your system when you first install it. For more information about using the ICE tools to modify your system configuration at a later date, see the Integrated Configuration Management section of the *Administration Guide for Cisco Unified Contact Center Domain Manager*.

Setup Servers

The Setup tab of the ICE Cluster Configuration tool displays setup wizards to configure the following cluster components:

- Unified CCDM Servers
- Cisco Unified CCE Servers
- Cisco Unified CM Servers

To start setting up your servers, in the Cluster Configuration tool, select the **Setup** tab in the left hand pane.

Setup Unified CCDM Servers

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

Note If you plan to use windows authentication to connect to the Unified CCDM database (rather than SQL authentication), you must have administrator permission on the database server on which the application is running.

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

To setup the Unified CCDM servers:

1. In the ICE Cluster Configuration tool, select the **Setup** tab and click **Setup UCCDM Servers** to start the wizard. Click **Next** to go through each window in turn.
2. In **Select Deployment Type** dialog box select your chosen deployment type. For more information on the supported deployment models of Unified CCDM please refer to section Deployment Models.
3. In **Configure Redundancy** dialog box select whether you would like to configure a single sided or a dual sided system. Click **Next**.
4. If you are performing a two tier deployment then you will be asked to enter the **Number of Web Servers** for each side. Enter the number of app/web servers for each side that you would like to configure in your deployment. For dual sided configurations you must configure an equal number of app/web servers on each side of the system. Click **Next**.
5. Click **Next**.
6. In the **Configure Servers** dialog boxes, enter the server names for each of the Unified CCDM servers. The number of dialog boxes and servers to specify will depend on the deployment options you chose above.
7. In each dialog box, enter the following:
   - Primary Server
     - **Sever Name**: This should be the non-domain qualified machine name.
     - **Server Address:** This is defaulted to **Server Name**. This may be changed to an IP Address or a domain qualified name of the server.
   - Secondary Server:
     - If you chose a dual sided setup, provide the details above for the Secondary Server (side B)
8. Click **Next** and enter the relevant server information until you reach the **Configure Relational Database Connection** dialog box.
9. In **Configure Relational Database Connection** enter the following details about how each Unified CCDM component connects to the Unified CCDM Relational database:
   - **Catalog:** This is the name of the Unified CCDM Relational database. The default is **Portal**.
   - **Authentication:** Select the authentication mode to connect to Unified CCDM relational database.

- **Windows Authentication.** The default recommended authentication mode.
- **SQL Authentication.** Only select this option if you are using a database server on a different domain. For this option you must enter your SQL Server Login Name and Password in the fields provided.

- Click **Next**.

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

Note Once you have made the required configuration changes, stop and restart all Unified CCDM services to ensure that all changes are propagated correctly. If you are planning to make other setup changes, you can wait until you have completed all your changes, and then stop and restart the Unified CCDM services once.

Configure Cisco Unified CCE Servers Wizard

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

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

Unified CCE Deployment Models

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

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

Unified CCDM Connection Requirements

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

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

Note

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

To configure the Cisco Unified CCE servers:

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

Note

The Modify and Remove options will only be enabled if there is at least one Cisco Unified CCE configured already.

3. In the Specify Resource Name dialog box, specify the name for the instance being configured. You can use the default name or choose another name.
4. In the Select Required Components dialog box, select the required components in the deployment.
   - **Admin Workstation**. This is a required component in all configurations.
   - **ConAPI Server (Provisioning)**. Check this option if you require resource management.
5. In the Configure Redundancy dialog box, select whether you want to configure a single sided or a dual sided setup.
6. In the Configure AW Servers dialog box, enter the following:
   - Primary Server:
     - **Sever Name**: This is the non-domain qualified machine name where the Admin Workstation and ConAPI components are deployed.
     - **Server Address:** This defaults to **Server Name**. This may be changed to an IP Address or a domain qualified name of the server.
   - Secondary Server:

- If you chose a dual sided setup, provide the details above for the Secondary Server (side B).

7. In the Configure Connection Details dialog box, enter the authentication details to connect to the Admin Workstation database.
   - **Windows Authentication**. This is the default recommended authentication mode.
   - **SQL Authentication.** If this mode is chosen then specify the SQL Server User name and the corresponding password to connect to the databases.
8. In the Select Unified CCE Instance dialog box select the AW instance to be used in the deployment. Click **Next**.
9. If you selected the **ConAPI Server (Provisioning)** option above then you will see the following dialog boxes:
   - In the Configure Primary ConAPI RMI Ports dialog box enter the following ConAPI details:
     - **Local Registry Port**. This is the port on the Unified CCE for the Unified CCDM Provisioning service to connect to. This will usually be 2099.
     - **Remote Registry Port**. This is the port on the Unified CCDM Database Server for the Unified CCE to connect to. This will usually be 2099.
     - **Local Port**. This is selected as the designated port for live provisioning traffic between the Unified CCE and Unified CCDM servers. It must be uniquely assigned for each Unified CCE and any firewalls between the CICM and Unified CCDM server must be configured to allow both-way traffic on this port.

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

   - In the Configure ConAPI Application Instance dialog box enter the following details:
     - **Application Name.** The name of the application to be used for provisioning Unified CCE from Unified CCDM. Specify the name of the application you configured in section Common ConAPI Credentials.
     - **Application Key.** Use the password for the application you specified above.
   - In the Multi Media Support dialog box, select **Yes** if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance to provide support for non-voice interactions. The default is **No**.
   - In the Purge On Delete dialog box select **Yes** if you want to purge items from Unified CCE automatically when they are deleted from Unified CCDM. The default is **Yes**.

- In the Self Skilling Enabled dialog box select **Yes** if you want to allow agents to reskill themselves. The default is **No**.
- In the WebView Support dialog box select **Yes** if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors. The default is **No**. If you select **Yes** then you will be prompted to provide Active Directory information so that Windows user accounts may be listed.

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

Note The **Configure Linked Unified CM Servers** window does not appear if no Unified CM servers are configured. You will be able to link the Unified CM servers to the Unified CCE from the Unified CM Configuration Wizard. You may also modify the Unified CCE once the Unified CM servers are configured and link the Unified CM later.

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

Configure Cisco Unified CM Servers Wizard

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

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

To configure the Cisco Unified CM servers:

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

- Remove an existing instance

Note: The Modify and Remove options will only be enabled if there is at least one Cisco Unified CM configured already.

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

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

Note: Redundancy is not supported for Unified CM configuration. The Secondary Server option is always disabled.

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

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

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

Configure Cisco Unified CVP Servers Wizard

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

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

Configuring a Cisco Unified CVP Call Server

To configure a Cisco Unified CVP call server:

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

Note The modify and remove options are only enabled if at least one Cisco Unified CVP call server has been configured.

3. In the Specify Resource Name dialog box, specify a name for the instance being configured. You can use the default value, or change it.
4. In the Configure Unified CVP Server dialog box enter the following:
   - Primary Server:
     - **Sever Name**: This is the non-domain qualified machine name where the Cisco Unified CVP Call Server component is deployed.
     - **Server Address:** This defaults to Server Name. You can change this to an IP Address or a domain qualified name of the server.

Note

The Unified CVP Call Server configuration does not support redundancy, so the Secondary Server option is always disabled.

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

Create CCDM Tenants and Map to Contact Center Equipment

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

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

Using the Equipment Mapping Tab

The Equipment Mappings page is divided into three vertical sections.

- Folder Tree section
- Source Equipment section (shown when an item is selected in the folder tree)
- Association Options section (shown when an item is selected in the source equipment section.

To configure your equipment mapping, in the Cluster Configuration tool, select **Equipment Mapping** in the left hand navigation pane.

Folder Tree Section

This section allows you to create new tenants and folders in the Unified CCDM Folder Structure. To create a new tenant or a folder, right click on the location in the tree where you would like to create the item and select **Add Tenant** or **Add Folder**.

Note

Tenants can only be created under the root folder. Folders can be created anywhere in the tree. A Tenant is a special folder that maintains ownership of an item. For example, in a hosted environment, the host's customers , map directly to individual

tenants, each of which is assigned their own individual resources, for example, Agents, Teams, Call Types etc.

Right clicking and selecting the **Refresh** option will refresh the folder structure from the database, reflecting any changes that may have been made through the Unified CCDM web application.

Source Equipment Section

This section lists all the configured source equipment. If none are configured then this list will be empty and you will not be able to do any associations.

When you select one of the items of configured equipment in the list, you will see options to map the resources belonging to that equipment to the selected folder in the **Association Options Section**.

Association Options Section

This section offers a list of association options between the folder or tenant in the folder tree and the source equipment.

- **Default Import Location**. Select this option to force the import to place all resources in the remote equipment into this folder or tenant.
- **Remote Tenant Mapping**. This option allows you to selectively associate dimensions based on remote ownership settings. Check an option to enable the drop-down list where the remote owner can be selected. After configuring a remote owner, all items owned by that owner on the remote equipment are imported to the selected folder or tenant.

Note The Remote Tenant Mapping is currently only valid for Cisco Unified CCE Resources. The list is populated with all the customer definitions available on the selected Cisco Unified CCE resource.

Creating Tenants and Folders

To create a Unified CCDM tenant:

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

To create a Unified CCDM folder:

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

Creating an Equipment Mapping

To create an equipment mapping between a tenant or folder and the Contact Center equipment:

1. In the ICE Cluster Configuration tool, select the **Equipment Mapping** tab. In the folder tree, select the tenant or folder into which you want to import the resources from the Contact Center equipment.
2. In the right hand pane select the check box next to the source equipment that you want to associate with the selected folder or tenant.
3. Select one of the following check boxes:
   - **Default Import Location -** all the resources imported from the source equipment will be placed in the selected folder or tenant in Unified CCDM.
   - **Remote Tenant Mapping** – all of the resources associated with the selected remote owner on the equipment will be placed in the selected folder or tenant in Unified CCDM.

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

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

Configuring Replication

In a dual sided Unified CCDM deployment setup, SQL Server Replication is used to replicate Unified CCDM databases. Replication between these databases is setup and monitored using the **Replication Manager** application which is available in the Unified CCDM Integrated Configuration Environment (ICE).

Note: The user running the Unified CCDM Replication Manager must have administrator permissions in both Windows and SQL Server, for both the targeted publisher and subscriber servers.

Note

Before configuring replication you should have already configured Unified CCDM resources in dual sided mode and saved the configuration using the **Cluster Configuration** tool detailed in section Configuring the Unified CCDM Cluster.

Note

Always run Replication Manger on the Unified CCDM publisher database server.

To start the Unified CCDM Integrated Configuration Environment, proceed as follows:

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

The Replication Manager offers two modes of operation; **Setup** and **Monitor**. Setup is used to configure or disable replication and Monitor is used to monitor the health of a configured Unified CCDM Replication.

Setup

Setup is used to configure or disable SQL Server Replication for the Unified CCDM databases in a dual sided environment. Click the **Setup** tab to see the replication setup details and to configure or disable replication as required by your deployment.

Setup is divided into three logical groups of property settings where some information may be modified if required.

Unified CCDM Database Server Properties

This section shows the configured Publisher and the Subscriber for Unified CCDM database. The **Server Name** and **Catalog Name** for each are defaulted to the values used when the Unified CCDM servers were configured with the ICE Cluster Configuration tool.

- **Server Name**: This is fixed for both the Publisher and Subscriber and cannot be changed from the Replication Manager. They rely on configurations made previously through the Cluster Configuration tool.

- **Catalog Name**: For both Publisher and Subscriber these represent the names of the respective Unified CCDM databases. The default values are those that were used when the Unified CCDM databases were configured using Cluster Configuration tool. It is recommended that the default be used.

Caution

If the Catalog Name for Publisher or Subscriber is changed, a Unified CCDM database with the new name must already exist on the respective server.

Distributor Properties

This section describes the properties for the SQL Server Replication Distributor. By default the Distributor is created on the Unified CCDM Database Subscriber Server.

- **Server Name**: This is the name of the subscriber server hosting the Portal database as configured using the Cluster Configuration tool.
- **Catalog Name:** This is the name that will be assigned to the distribution database. The recommended default is **distribution_portal**.
- **Data Folder**: This is the folder path on the distributor server where the data file for the distribution database will be created.
- **Log Folder**: This is the folder path on the distributor server where the transaction log file for the distribution database will be created.
- **Distribution Share**: This is the distribution share folder where replication snapshot files will be generated.
- **Override Distributor Admin Password**: When replication is performed an auto-generated password is used as part of the process to establish connectivity. The generated password is alpha-numeric with both upper and lower case characters. It will also contain a special character and will be 14 characters long. If the generated password does not meet with the complexity requirements of the server then check the check box and specify a password of your choice.

Note

In most cases the recommended defaults for these properties are valid and should be used. If you are performing an upgrade, be particularly careful with the Data Folder property, as the default path is different from previous versions. Make sure you use the path that you specified when the database was set up.

Configure or Disable Replication

Click **Configure** to start the replication configuration process. Progress messages will be logged into the Replication Output window informing you of the steps being performed as the DB is replicated.

If SQL Server Replication is already configured all of the controls will be disabled except the **Disable** button. Click **Disable** to disable replication. Progress messages will be logged into the Replication Output window.

Monitor

The **Monitor** tab allows you to monitor the general health of SQL Server Replication between Unified CCDM databases. The Monitor can also be used start or stop various replication agents. The Monitor will show the details only if SQL Server Replication is currently configured.

The top left pane shows the list of Publishers and Publications on each Publisher. If the Unified CCDM database is replicated then the following publications will be shown

- [Portal] Base
- [Portal] NonQueued

Click on a publication in the top left pane to see the corresponding subscriptions in the **Subscriptions** tab in the top right hand pane. The **Agents** tab lists other agents like Snapshot Agent, LogReader Agent and Queue Reader Agent if available for the selected publication. The list of agents depends on the Publication being viewed.

Click on the listed subscriptions or agents to see their session details in the bottom left pane. This pane will list all the agent sessions in the last 24 hours. Click on each session to see the actions performed during the session in the bottom right pane. This pane provides information about failures of any agents if any.

To stop or start the various replication agents, right click on the agent and select **Stop** or **Start** in the shortcut menu.

Note

By default, the Monitor refreshes every 5 seconds.

Configuring Unified CVP Media File Upload

Note

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

The 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 Unified CCE 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 CCDM and the Unified CVP Servers must belong to the same domain.

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 Server 2008.

Preparing the Configuration

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

1. Make a note of the Host Name and IP Addresses of ALL of the machines that are hosting Unified CVP.
2. 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.
3. 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. These instructions assume a Windows 2003 Domain Controller; for a Win 2008 DC, check with your Domain Administrators for details.

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

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

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

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 on the new root and select **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 CCDM 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 setup on all the machines to which the media files should be copied, and file replication enabled among all of them.

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

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

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.

6. Post Installation Steps

Securing Unified CCDM with SSL

Note

This step is optional. Follow the instructions in this section if you want to use Secure Sockets Layer (SSL) to secure Unified CCDM.

Introduction

To secure the Unified CCDM web servers using SSL you need to:

- obtain a digital certificate (see section Obtaining a Digital Certificate);
- configure SSL (see section Configuring SSL).

Obtaining a Digital Certificate

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

- purchased from an external certificate authority, for public use;
- generated internally, for secure use within the issuing organization;
- generated as a self-certified certificate, for local use (this option is not normally recommended except for testing purposes).

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

Note

Take care to specify the certificate name (common name, or friendly name, depending on the type of certificate) exactly as specified below. The certificate will not work otherwise.

1. Open **Internet Information Services (IIS) Manager** and select the web server in the folder hierarchy.
2. Select the **Features View** tab, and in the **IIS** group, click on **Server Certificates**.

3. Create a digital certificate in one of the following ways:
   - To *request an external certificate*:
     - In the **Actions** pane, select **Create Certificate Request** to display the **Request Certificate** dialog box.
     - In the **Common Nam**e field, enter the URL of the web server. If you have a load-balanced system, this must be the URL of the load-balanced node, not the URL of any of the individual servers.
     - Complete the other fields as appropriate, and click **Next**.
     - In the **Cryptographic Service Provider Properties** dialog box leave the default settings and click **Next**.
     - Specify a file name for the certificate, and then click **Finish**.
     - When you receive the certificate from the certificate authority, repeat steps 1 and 2 above to show the Server Certificates and Action panes, and in the **Action** pane, select **Complete Certificate Request.**
     - Enter the file name of the certificate, and a Friendly Name of your choice and click **OK**.
   - To *generate an internal certificate*:
     - Select **Create Domain Certificate** in the **Actions** pane to display the **Distinguished Name Properties** dialog box.
     - Enter the URL of the web server in the **Common Nam**e field. If you have a load-balanced system, this must be the URL of the load-balanced node, not the URL of any of the individual servers.
     - Complete the other fields as appropriate, and click **Next**.
     - In the **Online Certification Authority** dialog box specify your online authority and a friendly name. Click **Finish.**
   - To *generate a self-certified certificate*:
     - Select **Create Self-Signed Certificate** in the **Actions** pane to display the **Create Self-Signed Certificate** dialog box.
     - Enter the URL of the web server in the **Friendly Nam**e field. If you have a load-balanced system, this must be the URL of the load-balanced node, not the URL of any of the individual servers.

Configuring SSL

Once you have a suitable digital certificate, configure SSL as follows:

1. Open **Internet Information Services (IIS) Manager**, expand the folder tree below the web server and select the web site that the Unified CCDM web application resides on.

2. In the **Actions** pane, select **Edit Site** > **Bindings** to display the **Site Bindings** dialog box.
3. If there no existing binding for https, click **Add** to display the **Add Site Binding** dialog box.
   - Set the **IP Address** to **All Unassigned**, and **Port** to **443**, unless your system has been set up differently. If you are unsure, contact your system administrator.
   - Set **SSL Certificate** to point to your certificate.
   - Click **OK**.
4. If there is an existing binding for https, select it and click **Edit** to display the **Edit Site Binding** dialog box, edit the settings to the values in step 3 above and click **OK**.
5. In the folder tree, select the **Portal** application,
6. Select the **Features View** tab, and click on **SSL Settings** in the **IIS** group.
7. Tick **Require SSL**, and leave the default **Ignore** for Client Settings.
8. In the **Actions** pane, click **Apply** to apply these settings.
9. Close IIS Manager.
10. Go to **Start > All Programs > Domain Manager > Configuration Tools > Integrated Configuration Environment**.
11. The **Database Connection** window is displayed. In this window specify the following:
    - **Server Name** This option defaults to the current machine.
    - **Database Name** Select the Unified CCDM database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
    - **Authentication** Ensure this option is set to Windows Authentication.
12. Click **OK** to open ICE. The **Cluster Configuration** tool is open by default. Select the **System Properties** tool from the drop-down list.
13. Navigate to the **Global Properties** tab**, Report System Settings** group, **System URL** property, and change the start of the URL from `http://` to `https://`.
14. Click the **Save** icon, or select **File > Save** to save your changes.
15. Select **File > Exit**.

Securing CCDM Web Service APIs with SSL

Note

If you are planning to use the CCDM Web Services APIs then you must follow the instructions in this section to secure them with SSL. Otherwise you may ignore this section.

Introduction

The CCDM Web Services APIs allow you to customise CCDM by writing client code that accesses CCDM components programmatically. See the *Web Services Reference for Cisco Unified Contact Center Domain Manager* for more information about using the CCDM Web Services APIs.

The CCDM Web Services APIs are installed as part of the CCDM installation, and, by default are secured with a self-signed certificate called *localhost*. This certificate is suitable for a single server in a laboratory environment, but cannot be used to secure a multi-server installation in a production environment.

To secure the CCDM Web Services APIs using SSL you need to:

- obtain a digital certificate (see section Obtaining a Digital Certificate)
- grant network service rights to the certificate (see section Grant Network Service Rights to the Certificate)
- obtain the certificate thumbprint (see section Obtain the Certificate Thumbprint)
- configure Web Services to use the certificate (see section Configuring Web Services to use the Certificate)
- test the certificate installation (see section Test the Certificate Installation).

Obtaining a Digital Certificate

If you have secured CCDM with SSL as described in the section Securing Unified CCDM with SSL above, then you can use the same digital certificate to secure the Web Services.

Otherwise, if you do not already have a suitable certificate, you can follow the steps in the section Obtaining a Digital Certificate above to request or generate an external certificate (suitable for public use) or an internal certificate (for secure use within the issuing organization).

Grant Network Service Rights to the Certificate

To grant network service rights to the certificate:

1. In the Start menu, type **mmc** in the command box to open Microsoft Management Console (MMC).
2. Click **File > Add/Remove Snap-in**, click **Certificates**, then **Add.**

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

Obtain the Certificate Thumbprint

To obtain the certificate thumbprint:

1. In MMC, expand the Certificates node and the Personal node to see the available certificates and select the certificate you want to use.
2. Double click on the certificate.
3. In the Certificate dialog box, select the **Details** tab, and click **Thumbprint**. The thumbprint for this certificate is displayed on the lower part of the screen as a text string.
4. Select the thumbprint text string, copy it and paste it into a text editor. Edit the string to remove all the spaces. For example, if the thumbprint text string you copied was:

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

   you need to edit it to become:

   ```
   c3349a4328d3a775a993eb315cbfe062516db818
   ```

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

Configuring Web Services to use the Certificate

To configure Web Services to use the certificate:

1. Use Windows Services or the Service Manager in the ICE tool (See the *Administration Guide for Cisco Unified Contact Center Domain Manager*) to stop all CCDM services.

2. Remove the existing localhost certificates for each of the Web Services by typing the following commands at the command prompt:
   - subscription manager

     ```
     netsh http delete sslcert ipport=0.0.0.8083
     ```
   - notifications manager

     ```
     netsh http delete sslcert ipport=0.0.0.8084
     ```
   - resource management

     ```
     netsh http delete sslcert ipport=0.0.0.8085
     ```
3. Add the new certificates for each of the Web Services by typing the following commands at the command prompt, substituting the thumbprint value you obtained above instead of `<thumbprint>`:
   - subscription manager

     ```
     netsh http add sslcert ipport=0.0.0.8083 certhash=<thumbprint>
     appid={16dde36c-787e-4dc7-bdc0-fd4ae0eb189a}
     ```
   - notification manager

     ```
     netsh http add sslcert ipport=0.0.0.8084 certhash=<thumbprint>
     appid={16dde36c-787e-4dc7-bdc0-fd4ae0eb189a}
     ```
   - resource management

     ```
     netsh http add sslcert ipport=0.0.0.8085 certhash=<thumbprint>
     appid={16dde36c-787e-4dc7-bdc0-fd4ae0eb189a}
     ```

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

   ```
   netsh http add sslcert ipport=0.0.0.8083 certhash=
   c3349a4328d3a775a993eb315cbfe062516db818 appid={16dde36c-787e-
   4dc7-bdc0-fd4ae0eb189a}
   ```

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

Test the Certificate Installation

To test the certificate installation, in Internet Explorer, navigate to each of the links below, and check that the page opens without a certificate warning, and that the address bar shows a green safe status.

Configuring Single Sign-On

Overview

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

Note

Users cannot use SSO over a proxy connection.

Caution

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

Administrator Account Setup

Caution

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

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

You may now proceed to configure SSO for Unified CCDM.

Configuring SSO Authentication for Unified CCDM

1. From the location where you installed Unified CCDM (this will normally be **C:\Program Files\Domain Manager**), navigate to the **\Application Server** folder.
2. Open the XML file **Exony.Reporting.Application.Server.exe.config**.

Note

Some text editors, such as WordPad, will not save an XML file correctly, which may cause problems. Always back up the config file before making changes.

3. Locate the following section:

```
<Exony.Reporting.Application.Security.Security>
      <setting name="Authentication" serializeAs="String">
            <value>Portal</value><!--SSO|Portal-->
      </setting>
</Exony.Reporting.Application.Security.Security>
```

4. Change `Portal` to `SSO`

```
<Exony.Reporting.Application.Security.Security>
            <setting name="Authentication" serializeAs="String">
                  <value>SSO</value><!--SSO|Portal-->
            </setting>
</Exony.Reporting.Application.Security.Security>
```

5. Save and close.
6. Run **services.msc** and restart the Unified CCDM Services (Scheduling, Reporting, Search, Monitoring etc).
7. Open **Internet Information Services (IIS) Manager** and select **Sites > Default Web Site**.
8. Select the **Portal** virtual directory, choose the **Content View** option. Locate the **post_logon.aspx** file.
9. Right-click **post_logon.aspx** and select **Switch to Features View**.
10. Double click on the **Authentication** option and ensure that **Anonymous Authentication** is disabled and **Windows Authentication** is enabled. Disable all authentication providers except **Windows Authentication** and **Forms Authentication**.
11. **Close Internet Information Services (IIS) Manager.**
12. From the location where you installed Unified CCDM (this will normally be **C:\Program Files \Domain Manager**), right-click on **Web** folder and click **Properties**.
13. In **Security** tab, click **Advanced** and ensure that the **Allow inheritable permissions from the parent** to propagate to this object and all child objects option is checked
14. Give **Read** and **Read & Execute** properties on the Web directory to all domain users who should have access to Unified CCDM.

Note To avoid performing this step for each new user, you can create a *Unified CCDM Users* group and add new users to this group as required.

15. Click **OK** to close the Advanced Security Settings and Web Properties windows.
16. Double-click **Web** folder and open **web.config** file.
17. Locate the following section:

```
<setting name="AuthenticationProvider" serializeAs="String">
             <value>Portal</value><!--SingleSignOn|Portal-->
```

18. Change `Portal` to `SingleSignOn`:

```
<setting name="AuthenticationProvider" serializeAs="String">
             <value>SingleSignOn</value><!--SingleSignOn|Portal-->
```

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

You will now be able to access Unified CCDM from your domain account without logging in.

Managing Users with Single Sign-On

Once SSO has been set up, all Unified CCDM users must be given a Unified CCDM login in the form `<DOMAIN>\<Windows domain login>`. This means that previously-existing Unified CCDM user accounts must be recreated in the new format before any users can login.

Each time a new user is given a Unified CCDM account, that user must either be given Read and Read & Execute properties on the Web directory as described above, or added to a user group that has those permissions.

Each new user will also need to add Unified CCDM to their list of trusted sites in Internet Explorer.

Performance Configuration Checklists

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

Web Server

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

Database Server

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

System Reset

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

Logging into Unified CCDM

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

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

System Checks

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

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

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

This query should return a value of at least 3.

7. Uninstalling Unified CCDM

This chapter describes how to remove the Unified CCDM components from the platform. The uninstallation procedure should be performed in the following order:

Uninstalling Database Components

This process will remove the database components. This removes the ability to import and provision data between remote data sources (such as Unified CCE or Unified CM) and the Unified CCDM Database.

Removing Database Replication

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

Note Removing database replication may take some time.

Before removing database replication:

- Ensure that you are logged in as a domain level user with administrative rights on both database servers.
- Ensure that the database is in a consistent state
- Stop all Unified CCDM Services on all servers.

To disable replication:

1. Click **Start > All Programs > Domain Manager> Configuration Tools > Integrated Configuration Environment**.
2. In the **Tools** drop-down, select **Replication Manager**. The Replication Manager tool is displayed.
3. Select the **Setup tab**.
4. Click **Disable**.

Once replication is disabled you can uninstall the database components as described in the next section.

Uninstalling Database Components

To uninstall the database components:

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

Note

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

Removing the Database Catalog

Caution

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

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

1. Click Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio
2. Connect to the local database server.
3. In the Object Explorer pane, expand the Databases node, navigate to the Unified CCDM database (the default name is Portal), right click it and select **Delete**.
4. The Delete Database window displays.
5. Select the **Close existing connections** check box.
6. Click **OK**.

This permanently removes the database catalog.

Uninstalling Other Components

All the other Unified CCDM components may be uninstalled by clicking **Remove** from **Add/Remove Programs**.

8. Troubleshooting

Installer Logs

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

Adding a New Web Server after the Database has been Installed

If you need to recover or expand your system, you may need to install a new web server. Under normal installation conditions the details of the web server are known at install time and can be provided during the database installation so that suitable permissions for access to the database from the web server's Network Service account can be applied by the installer. Adding a web server to the cluster at a later date requires permissions to be set up manually for the Web Server's Network Service Account on the Portal database.

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

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

- db_datareader
- db_datawriter
- db_ddladmin
- db_securityadmin
- portalapp_role
- portalreporting_role
- portalrs_role

8. Click **OK.**