Installation and Configuration Guide for Cisco Unified Contact Center Domain Manager

Release 11.6

Updated July 2019

Table of Contents

Preface

Purpose

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

Audience

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

Organization

The sections of this guide are as follows:

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

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

Document Conventions

This document uses the following conventions:

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

Obtaining Documentation and Submitting a Service Request

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

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

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

Field Alerts and Field Notices

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

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

Documentation Feedback

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

We appreciate your comments.

Planning Your Installation

About Your Installation

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

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.

Infrastructure Software

Unified CCDM requires:

- Windows 2012 Server R2
- SQL Server 2014 64-Bit, Standard Edition, Service Pack 2.

Unified CCDM Components

A Unified CCDM installation comprises the following components.

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

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

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

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

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

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

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

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

  - **Identity Server**, which provides a two factor identification system that allows implementation of single sign-on, and access control. The lightweight authentication service includes Local, Windows, and ADFS authentication. Users can have mixed authentication modes, which define how a user can access the system.

Deployment Models

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

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

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

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

Figure 1.1 "Component Layout for a Dual Tier Deployment" below, describes the software installation layout for dual tier deployment. The web server and application server components reside on a separate server. This configuration can optionally have a second side in the same configuration for resilience.
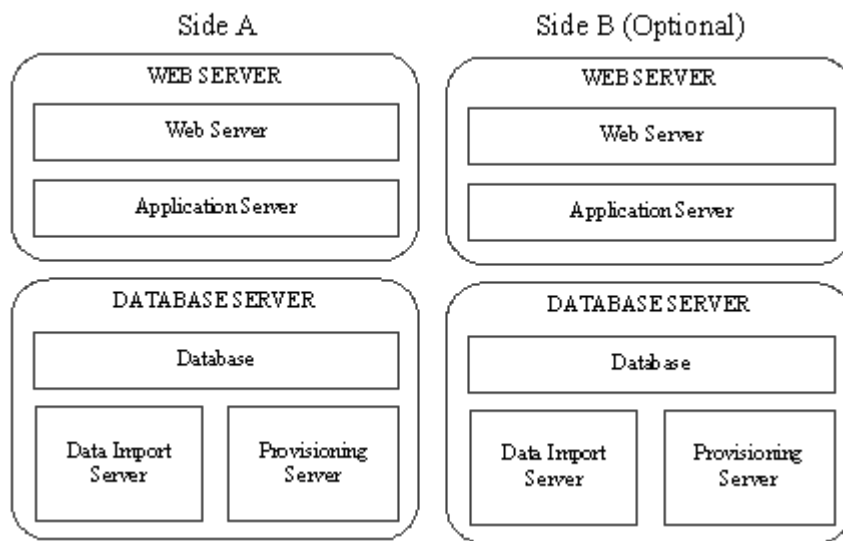
Figure 1.1   Component Layout for a Dual Tier Deployment

Installation Requirements

About the Installation Prerequisites

This section describes the installation prerequisite requirements for Unified CCDM.

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

General Requirements

This section describes the general requirements for your installation.

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

Windows Requirements

All Unified CCDM servers require the following version of Windows:

- Windows Server 2012 R2.

Additional Software Requirements

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

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

Database Servers

The Unified CCDM Database Server will require Microsoft SQL Server 2014 64-bit, Standard Edition. The following components should be deployed:

- Database Engine.
- Workspace Components.

Application Servers

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

Clients running the Web Application

The Unified CCDM web application supports the following browsers:

- Google Chrome version 49.0.2623 m
- Internet Explorer version 11 (Windows 7 or Windows 8.1)
- Mozilla Firefox versions 45.0.1 (Windows 7, Windows 8.1, or Mac).

Note. The Unified CCDM web application may not work with virtual desktops or application virtualiztion technologies (for example, Citrix XenDesktop, Citrix XenApp, VMware Horizon View). You may use these technologies but we cannot provide support in the event of a problem, unless the issue can be replicated using one of the supported browser configurations.

Firewall Configuration

About Firewall Configuration

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

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

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

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

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

Web Server Port Usage

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

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

Unified CCDM Database Server Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Servers Requiring Access	Usage
SQL Server	TCP	1433	Other Database Servers, Application Servers	General
DTC	TCP	2103	Other Database Servers	Audit Archive
DTC	TCP	2105	Other Database Servers	Audit Archive
DTC (RPC)	TCP	135	Other Database Servers	Audit Archive
DTC (RPC)	TCP	5000-5100*	Other Database Servers	Audit Archive
NetBIOS File Share	UDP	137-138	Other Database Servers, Application Servers	Replication, Unified CVP File Upload
NetBIOS File Share	TCP	139	Other Database Servers, Application Servers	Replication, Unified CVP File Upload
SMB (DFS)	TCP	445	Other Database Servers, Application Servers	Unified CVP File Upload File**
ConAPI Local Registry	TCP	2099***	Unified CCE Admin Workstation	Provisioning
ConAPI Local Port	TCP	3333***	Unified CCE Admin Workstation	Provisioning
ConAPI Local Port	TCP	3334****	Unified CCE Admin Workstation	Provisioning (Dual-sided deployments only)

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

    HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet

After each change the machine must be restarted.

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

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

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

Cisco Unified CCE Port Usage

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

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

Domain Controllers for Unified CCE Instances Port Usage

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

Cisco Unified CVP Port Usage

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

Other Information

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

* Distributed Transaction Coordinator
* File and Printer Sharing.

Security Considerations

Mandatory Security Configuration

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

You must:

- Configure Secure Sockets Layer (HTTP) for the Unified CCDM web application (see section "Configure SSL" for instructions).

Recommended Security Configuration

This section describes the steps that are strongly recommended to secure your system. Detailed instructions are provided at the appropriate point in the installation instructions. If you omit any of the steps in this section, your installation may be vulnerable to attack.

It is strongly recommended that you:

- Disable SSL v3 for the Unified CCDM web application (see section "Disable SSL3 V3"for instructions). This helps prevent "man in the middle" attacks that could intercept data that is encrypted using SSL v3. For more information, see http://en.wikipedia.org/wiki/POODLE (link checked November 2014).

Optional Security Configuration

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

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

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

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

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

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

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

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

- Remove the "aspnet_client" folder, which is installed with .Net, typically in the C:\inetpub\wwwroot folder. This folder appears by default on an IIS Server, but is not used by Unified CCDM.

Windows and SQL Installation and Configuration

Windows Configuration

Firewalls

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

All Unified CCDM Servers

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

   - configure the server to use the US English character set

   - configure Microsoft Terminal Services for remote configuration and support

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

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

SQL Server

Install SQL Server

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

On the Side A server:

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

2.   Select **New SQL Server stand-alone installation or add features to an existing installation**.

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

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

5. The **Global Rules** window displays, validating the system for the SQL Server installation. Once validation passes, click **Next**.

6. Ensure that Microsoft updates are not selected, then click **Next**.

7. The installation of setup files starts, then the system setup is validated. Once validation is completed, click **Next**.

8. Select **Perform a new installation of SQL Server 2014**, then click **Next**.

9. In the **Setup Role** window, select **SQL Server Feature Installation** and click **Next**.

10. In the **Feature Selection** window, select the following instance features:

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

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

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

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

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, set the **Account Name** to **NT AUTHORITY\SYSTEM** and the **Startup Type** to **Automatic**.

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

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

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

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

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

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

- Click **Next** to proceed.

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

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

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

20. When the SQL Server 2014 installation is complete, locate and install SQL Server 2014 Service Pack 2.

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

Configure SQL Server Network Protocols

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

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

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

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

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

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

6. Close the SQL Server Configuration Manager window.

Configure Windows Firewall for SQL Server

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

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

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

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

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

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

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

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

8. Close the Server Manager window.

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.

User Accounts

Unified CCDM Service Accounts

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

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

SQL Agent User

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

Notes

The domain account for the **sql_agent_user** needs to have write permission to the SQL Server common files folder COM. The default folder is **<Install Drive>:\<Program Files>\Microsoft SQL Server\<SQL Version>\COM**, where:

•   **<Install Drive>** is the drive letter of the drive SQL Server was installed on.

•   **<Program Files>** is the folder that SQL Server was installed to.

•   **<SQL Version>** is the version number for the SQL Server common folder.

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

To create the required account:

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

   - Password never expires
   - User cannot change password.

Optional Security Configuration

Disable SSL3 V3

Caution!

This step concludes by rebooting the App/Web server automatically. Please ensure you have saved your work before continuing.

Note

This step is optional, but it is strongly recommended for maximum security. See section "Security Considerations" for more information.

Some of the other security configurations in this section also require a server reboot, so if you are applying those too, you may want to make this step the final one.

On each App/Web Server:

1. In Windows Explorer, open the folder below the Unified CCDM installation containing the **Hardy** security tool. If you have used the default installation location, this will be **C:\Program Files\Domain Manager\Hardy**.

2. Double click on the Hardy executable to run it. The name of the file to choose depends on whether you have kept or changed the default Windows folder option **Hide extensions for known file types**:

   - if extensions for known file types are hidden, choose **Exony.Portal.Tools.Hardy**. Do not choose **Exony.Portal.Tools.Hardy.exe** (which is an XML configuration file).

   - if you have opted to show extensions for all file types, choose **Exony.Portal.Tools.Hardy.exe**.

3. The server will reboot automatically.

Disable Anonymous Sessions

Note

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

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

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

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

then enable the setting

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

Alternatively, you can update the registry directly as follows:

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

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

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

4.   Close the registry editor.

Disable Cached Logins

Note

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

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

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

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

then set the following setting to **0**

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

Alternatively, you can update the registry directly as follows:

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

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

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

4.   Close the registry editor.

Disable DCOM

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

This security setting applies to all Unified CCDM servers.

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

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

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

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

Enable Mandatory SMB Signing for all Unified CCDM Servers

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

This security setting applies to all Unified CCDM servers.

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

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

3.   Close the Local Security Policy dialog box.

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

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

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

Disable SSL V2

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

On each App/Web Server:

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

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

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

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

5. Close the registry editor and reboot the server.

Disable Remote Access to Unified CCDM Servers

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

Unified CCDM Installation

Before You Start

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

Installing Dual-Sided Systems

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

Recording Your Settings

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

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

The Unified CCDM Installer

About the Unified CCDM Installer

Starting the Installer

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

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

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

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

Note

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

Installation Prerequisites

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

Where possible, the Unified 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.

Install the Database Components

On the Side A Database Server:

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

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

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

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

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

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

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

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

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

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

    > **Warning**
    >
    > The cryptographic passphrase is a vital piece of information and will be needed when installing later components and when adding or replacing servers in the future. Be sure to record and retain it.
    >
    > If you are upgrading from a previous version of Unified CCDM, or adding a new server to an existing cluster, you must use the same cryptographic passphrase as was originally used. If you continue the installation with a new passphrase you will be unable to access your existing data.

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

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

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

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

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

    - Click **Next**.

9.   In the **Destination Folder** window, if you want to change the location where the database components are stored, click **Change** and select the new location. The Unified CCDM components need to be installed in the same directory location on each of the servers.

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

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

12.   Click **Finish**.

Install the Portal Database

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

To install the portal database:

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

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

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

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

 • **Server Name**. Enter the name of the machine that is to be the Database Server. This should normally be left as the default (**localhost**). Logon for the SQL Server service needs full control over the folder (or the individual files in the folder) that contains the database files. The folder that you put the SQL database files into cannot be compressed.

 • **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 components. If not, you will see a warning message.

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

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

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

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

- Click **Next**.

5. In the **Optimize System Databases** window, you can change the configuration of the Unified CCDM database file groups and files to improve performance, if required. All file groups will automatically be split in to multiple files on the drive based on the number of logical processors on system divided by 4. You can reconfigure your database files manually after completing the installation.

   For optimum performance, it is recommended that **TempDB** is not installed on the same disk as the operating system.

   - **To split a file group**, choose the **Split** option, click the drop-down arrow to filter the list of file groups by database, select the file group or file groups you want to split, then click **Go**. The selected file group or file groups will be split into the optimal number of files for your server configuration (one file for every two logical CPUs).

   - **To move a file**, choose the **Move** option, click the drop-down arrow to filter the list of files by database, select the file or files you want to move, click **Location** to select the new location, then click **Go**. The selected file or files will be moved to the new location.

   - When you have made the changes you require, click **Next**.

6. 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**.

7. 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 clear **Set Initial Size to Max Size**.

- To enable or disable the new minimum file size limit of 15mb, select the **Enable/Disable Minimum File Group Sizes** check box.

- 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.

Note

After the size of the database has been set, the system calculates the recommended size of the TempDB and TempDBLog sizes. It is recommended that the file sizes be adjusted to the recommended values in SSMS.

If the database is bigger than the size allocated to the PortalLog file, a warning will be displayed. You can choose to ignore it, or to go back and specify a different size.

8. The **Configure Local Administrator Details** window sets the identity details for the default administrator account:

- **Account Type**. The type of user account that will be used. This is set to **Administrator** and cannot be changed.

- **Password**. Enter a password for the administrator, conforming to your individual system's complexity requirements.

Note

This password cannot be retrieved or reset.

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

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

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

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

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

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

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

- Click **Next**.

10. In the **Configure the Location of the Identity Data Files** select the location of the identity data files.

    - To change the location, click **Location**.

    - Select the location of each file group.

    - Click **OK** to save your changes.

    - Click **Next** when you have selected the location for each file group.

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

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

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

Install the App/Web Server

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

On the Side A App/Web Server:

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

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

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

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

5.   If the **Domain Manager: Application Server Components** dialog is displayed, click **Install** to install the additional required components.

6.   If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.6 Framework is complete, restart the server to continue the installation of the App/Web Server.

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

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

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

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

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

    •   Click **Next** to continue.

> **Warning!**
>
> You must use the same cryptographic passphrase for all servers in the Unified CCDM installation. If you continue the installation with a new passphrase you will be unable to access your existing data.

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

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

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

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

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

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

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

- Click **Next** to continue.

11. Click **Install**.

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

Install the Identity Server

Install the new Identity Server components. Ensure that you have successfully installed the App/Web Server before attempting to install the Identity Server.

1. Start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see section "About the Unified CCDM Installer").

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

3. When all checks have passed, click **Install** to begin the Identity Server installation.

4. 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.

5. In the **Destination Folder** window:

   - Click **Change...** to browse to the destination folder you want to install into.

6. In the **Ready to install Identity Server** window, click **Next** to begin installation. Installation will take several minutes.

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

Load Balancing the Identity Server

These extra steps are required if the solution is going to use a load balancer to serve multiple identity or web servers.

Notes

Without these steps, logins may fail if requests are sent to the Identity Server using a different database from the first part of the login flow - replication can not happen that quickly.

If you are using a load balancer then the URL must be used in the eGain Analytics setup ICE wizard - the web server machine names should not be used. This means a load balancer needs to be setup before configuring eGain Analytics.

Step 1: Share the same signing certificate

1. On Side A, export the signing certificate (including the private key) that is being used. By default the signing certificate is called "**idsrv3**". If a custom certificate is being used, the web.config file enables you to configure the name using a subject name or a thumbprint under setting **svr.signingCertificate**. The **svr.signingCertificate** setting can be either:

    *   CN=somename
    *   somethumbprint.

    Warning!

    If you are using a custom certificate, please ensure that only **one** certificate with the same subject name exists on the machine. You can use a thumbprint rather than a subject name to avoid duplicates.

2. On Side B, import the signing certificated certificate. You will need to update the identity server web.config ("**D:\Program Files\eGain Analytics\Identity Server\Identity.Server\web.config**") if a custom certificate is used. You will also need to give NetworkService Read permissions to the private key. To do this:

    *   Click **Certificate**, and then **All Tasks**.
    *   Select **Manage Private Keys**.

Step 2: Ensure identity server affinity

To ensure that the web application uses the same server as the incoming client request the load balancer URL must resolve on the web server to itself. To do this:

1. Edit the web server host file "**C:\Windows\system32\drivers\etc\hosts**" to resolve the load balancer hostname to the loopback ip address "**127.0.0.1 awww.loadbalancer.com**".
2. Import the SSL certificate and private key (PFX file format) used on the load balancer.
3. Add the SSL certificate to the Local Machine personal store. This must be done even if the load balancer is doing SSL-Offloading.
4. Within IIS Manager, change the Bindings so that port 443 is using the newly imported load balancer SSL certificate.

5.   Restart IIS.

These steps now apply the web application to use the loadbalancer URL for its own internal requests during logins. This means the web application will correctly use the Identity Server running on the same physical machine.

Install the Second Side (Replicated Systems Only)

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

Support Tools

About the Support Tools

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

Install the Diagnostic Framework

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

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

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

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

- Click **Next**.

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

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

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

- Click **Next**.

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

6.   Click **Install**.

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

The installation of the Diagnostic Framework component is now complete.

Unified CCDM Configuration

About Unified CCDM Configuration

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

This section describes the following steps:

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

Configure Active Directory Federation Services (ADFS)

About ADFS

By default, Unified CCDM users need to log in to Unified CCDM every time they connect. Unified CCDM can optionally be configured to use ADFS, which links each Unified CCDM user account to their ADFS user account and enables users to connect to Unified CCDM without logging in.

This section provides information on how to configure the ADFS application. To use ADFS to login to Unified CCDM, it is necessary to map it to the Identity Server within Unified CCDM.

Configure ADFS per identity server

To manually add the Unified CCDM identity server to ADFS:

1. Open **AD FS Management**.
2. Open **Trust Relationships**, and **Relying Party Trusts**
3. Select **Add Relying Party Trust...**. The Add Relying Party Trust Wizard opens. Click **Start**.

4. Select **Enter data about the relying party manually**, then click **Next**

5. Enter an appropriate display name, for example "Unified CCDM Identity Server", then click **Next**.

6. Select **AD FS profile**, then click **Next**.

7. Click **Next**, as Unified CCDM do not support an optional token encryption certificates.

8. Select **Enable support for the WS-Federation Passive protocol**, and enter the full URL to the identity server ADFSendpoint.

> **Note**
>
> The URL must use a SSL certificate that ADFS trusts, and must be in the correct format.
>
> For example, "https://webapphostname/Identity/adfs".

9. Under **Relying party trust identifier**, enter the full URL to the identity server. Click **Add**, then **Next**.

10. Select **I do not want to configure multi-factor authentication settings for this relying party trust at this time**, and click **Next**.

11. Select **Permit all user to access this relying trust party**, and click **Next**.

12. Review the settings. You can go back and change any settings, or, if you are happy with the current settings, click **Next** to add the relying party trust to the ADFS configuration database.

13. Select **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** if you want to edit claim rules immediately.

14. Click **Close** to exit the wizard.

To edit the claim rules for Unified CCDM:

1. Open **Trust Relationships**, and **Relying Party Trusts**.

2. Select the Unified CCDM trust, and click **Edit Claim Rules...** to open the Edit Claim Rules dialog.

3. Select the **Issuance Transform Rules** tab.

4. For each of the below **Claim Rules**, click **Add Rule**, select **Send LDAP Attributes as Claims** and complete the Add Transform Claim Wizard.

Claim Rule Name	Store	LDAP Attribute	Outgoing Claim Type	Mandatory
AD: SID as NameID	Active Directory	objectSid (type directly)	Name ID	Yes
AD: UPN as Name	Active Directory	User-Principal-Name	Name	Yes
AD: GivenName (optional)	Active Directory	Given-Name	Given Name	Optional
AD: Surname (optional)	Active Directory	Surname	Surname	Optional
AD: Email (optional)	Active Directory	E-Mail-Addresses	E-Mail Address	Optional

Note

It is recommended that you use a System Identification Number (SID) as NameID, as it is necessary for the NameID to be unique to each user.

5.   Once the claims have been setup, click **Finish** the close the dialog.

6.   Alternatively, if you wish to support automatic user provisioning:

  •   Click **Add Rule** to add a new claim.

  •   Select **Send Group Membership as a Claim** as the claim rule template, and click **Next**.

  •   Enter the following additional claim rules.

Claim Rule Name	User's Group	Outgoing Claim Type	Outgoing Claim Value
AD: Role = Supervisor	<windows group>	Role	Supervisor
AD: Role = Advanced	<windows group>	Role	Advanced

7.   Once the additional claims have been setup, click **OK** the close the dialog.

Configure ADFS as a one time setup

A one time setup configuration of ADFS is only required if you want to support automatic user provisioning. As a one time step (not per identity server), you need to add a custom rule to allow Unified CCDM to map tenants to ADFS.

1. Open **AD FS Management**.

2. Select **Trust Relationships** > **Claims Provider Trusts**.

3. Select **Active Directory**, and **Edit Claim Rules**. The Edit Claim Rules for Active Directory dialog box opens.

4. Click **Add Rule...**.

5. Select the **Send LDAP Attributes as Claims** claim rule template. Click **Next**.

6. Type in "Pass-thru DN" as the **Claim Rule name**.

7. Select Active Directory as the **Attribute Store**.

8. Map the following:

LDAP Attribute (Select or type to add more)	Ongoing Claim Type (Select or type to add more)
distinguishedname	http://temp.org/claims/DistinguishedName

9. Click **Finish** to save the claim rule for Active Directory.

Once you have set up ADFS to support automatic provisioning, you can map tenants to ADFS

Once you have configured ADFS, you must restart the Unified CCDM server for the changes to come into effect.

To map tenants to ADFS

It is only required to map tenants to ADFS if you want to support automatic user provisioning.

1. Select the Unified CCDM trust, and click **Edit Claim Rules...** to open the Edit Claim Rules dialog.

2. Select the **Issuance Transform Rules** tab.

3. To add claims, click **Add**. The Add Transform Claim Rule Wizard opens.

4. Select **Send Claims Using a Custom Rule** as the claim rule template, and click **Next**.

5. Enter the claim rule name in the format:

    AD: Tenant(<TenantPath>)

6. Enter Custom rule text in the format, with the values you want to use:

c:[Type == "http://temp.org/claims/DistinguishedName", Value =~ "^.*()$"]

=> issue(Type = "http://egain.net/claims/identity/tenant", Value = "/");

7.   Click **Apply**.

8.   Click **Finish** to close the dialog.

Configure Windows Login

About Windows Login

By default, Unified CCDM users need to log in to Unified CCDM every time they connect. Unified CCDM can optionally be configured to use Windows, which links each Unified CCDM user account to their Windows user account and enables users to connect to Unified CCDM without logging in.

Set Up Administrator Account

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

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

- The login name must correspond to an existing Windows Active Directory user, and must be formatted as **<username\domain-name>**, where **<username>** is the Windows username and **<domain-name>** is the NetBIOS domain name. The login name must exactly match the details in the corresponding Active Directory entry,

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

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

4.   Click **Add to Group**.

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

6.   Close and save.

Configure Windows Authentication

To configure Windows for Unified CCDM, on the Database Server:

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

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

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

- **Authentication**. Select any authentication configured on the database.

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

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

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

5. On the App/Web Server, go to the location where Unified CCDM was installed (usually **C:\Program Files\Domain Manager**), right-click the **Web** folder and select **Properties**.

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

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

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

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

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

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

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

    For example, if your web URL for the Unified CCDM web application is `https://mycompany/portal` and the name of your Unified CCDM App/Web Server is `Unified CCDMWeb1`, you would enter

    ```
    setspn -a http/mycompany Unified CCDMWebfqdn
    ```

    Reboot the Unified CCDM App/Web Server or servers.

You have now configured Windows and users will be able to access Unified CCDM directly from their domain account without needing to login again.

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

Manage Users with Windows

Login names for new users should be in the **<username>\<domain-name>** format, for example, **user1@testdomain.local**.

> **Note**
>
> Unified CCDM Users located on an external domain from the Unified CCDM hosting domain require a trust relationship to be configured between the hosting and external domain.

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

Configure Unified CCE Admin Workstations

Unified CCDM database server(s) requires access to the Admin Workstation database to import data resource information.

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

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

2. Launch **SQL Server 2014 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 Servers), by filling in the fields as follows:

    • **General** page:

- **Login Name**: Enter the machine name (or the windows service account name) in the form **<DOMAIN>\<MACHINENAME>$**, for example **ACMEDOM\ACMESERVER1$** where ACMESERVER is the Unified CCDMdatabase server. This configures access for the NETWORK SERVICE account from the Unified CCDM database servers. On dual-sided deployments, both Unified CCDM database servers must have machine accounts set up.

        - **Authentication**: Select Windows Authentication unless connecting to a server on a different domain

    - **User Mapping** page:

        - **Users mapped to this login**. Select AWDB.

        - **Database role membership for**. For AWDB, select **Public** and **db_datareader**.

6.   Click **OK**.

Configure Unified CCE Provisioning

About Provisioning Configuration

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

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

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

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

    - ConAPI only supports connection to one Application Instance on each physical server. You must therefore have a separate physical AW distributor for each instance.

    - Parent/Child AW configurations are supported as multiple instances in Unified CCDM.

Note

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

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

Set Up ConAPI

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

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

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

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

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

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

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

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

    *   **Application Type**: Select **Cisco Voice.**

    *   **Permission Level**: Give the application full read and write permissions.

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

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

Set Up the CMS Server

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

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

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

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

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

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

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

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

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

    - **Application RMI registry port**. The port on the Unified 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 specified above. Each Unified CCE AW must connect to a different port on the Database Server. You should record this information for future use.

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

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

Configure the Unified CCDM Cluster

About Cluster Configuration

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

- configure the servers in the Unified CCDM cluster (the Unified CCDM servers, Unified CCEs and Unified Communications Managers)

- set up the equipment mappings between remote tenants and Unified CCDM resources.

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

Start ICE Cluster Configuration

To start ICE, on the Side A Database Server:

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

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

   - **Database Name**. Enter the name of the Unified 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.

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

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

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

Set Up Unified CCDM Servers

About the Setup Unified CCDM Servers Wizard

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.

Setting Up the Unified CCDM Servers

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

To set up the Unified 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. On the **Select Deployment Type** page, select your chosen deployment type.

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

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

5.   On the **Configure Servers** pages, enter the server names for each of the Unified CCDM servers. The number of pages and servers to specify will depend on the deployment options you chose above. The database catalog name for the Identity Server is fixed to IdSvr3Config.

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

   •   **Primary Server**

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

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

      •   **FQDN Web Url**. The Fully Qualified Domain Name used to access this web application server. The FQDN will depend on the method of access to the application website, based on whether it is with or without load balancer. With load balancer, the FQDN will be the load balancer FQDN and must be specified in all Configure Application Server pages. Without load balancer, this will be the FQDN used to access each website separately.

   > **Note**
   >
   > The FQDN must match the SSL certificate.

   •   **Secondary Server**

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

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

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

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

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

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

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

- Click **Next**.

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

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

- **Catalog**. This is the name of the Unified CCDM database. The default is **Portal**.

- **Authentication**. Select the authentication mode to use to connect to the Unified CCDM database.

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

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

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

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

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

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

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

Configure Cisco Unified CCE Servers

About the Configure Cisco Unified CCE Servers Wizard

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

- add a new Cisco Unified CCE instance to the deployment

- update an existing Cisco Unified CCE instance in the deployment

- remove an existing Cisco Unified CCE instance from the deployment.

About Unified CCE Deployment Models

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

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

About Unified CCDM Connection Requirements

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

* Unified CCE real-time AWDB for data import

* Unified CCE AW for Unified CCDM Provisioning Server requests.

Configuring Cisco Unified CCE Servers

Note

This wizard configures the Unified CCE servers using an SQL Connection. You will need to
know the connection credentials to complete the configuration.

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

To configure the Cisco Unified CCE servers:

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

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

   * Add a new instance

   * Modify an existing instance

   * Remove an existing instance.

Note

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

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

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

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

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

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

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

  - **Primary Server**:

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

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

  - **Secondary Server**:

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

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

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

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

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

9. On the **Configure Primary Unified Config Web Service** page, (only shown if the Unified CCE instance is running Unified CCE version 10.5 or later), enter the following details

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

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

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

> **Note**
> If the user permissions are changed then we need to start "Apache Tomcat" service on UCCE.

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

- **Local Registry Port**. This is the port on the Unified CCE for the Unified 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 page.

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

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

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

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

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

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

> **Note**
>
> A two way trust relationship is required between Unified CCE and CCDM.

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

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

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

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

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

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

Configure Cisco Unified Communications Manager Servers

About the Configure Cisco Unified Communications Manager Servers Wizard

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

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

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

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

Configuring Cisco Unified Communications Manager Servers

To configure the Cisco Unified Communications Manager servers:

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

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

      *   Add a new instance

      *   Modify an existing instance

      *   Remove an existing instance

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

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

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

-    **Primary Server**

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

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

Note

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

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

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

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

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

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

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

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

Note

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

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

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

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

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

Configure Cisco Unified CVP Servers

About the Configure Cisco Unified CVP Servers Wizard

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

This wizard guides you through the steps to:

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

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

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

Configuring Cisco Unified CVP Servers

To configure a Cisco Unified CVP server cluster:

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

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

   * Add a new instance

   * Modify an existing instance

   * Remove an existing instance.

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

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

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

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

   * **Primary Server**:

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

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

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

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

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

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

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

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

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

8. If you specified at least one call server:

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

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

    - **Primary Server**:

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

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

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

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

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

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

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

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

Create and Map Tenants

About Creating and Mapping Tenants

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

* create the Unified CCDM folder structure for your deployment

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

Creating Tenants and Folders

To create a Unified CCDM tenant:

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

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

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

To create a Unified CCDM folder:

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

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

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

Creating an Equipment Mapping

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

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

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

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

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

- **Customer Resource Mapping**. Allows more control over the import process. You can specify the items on the highlighted contact center equipment to be placed in the selected folder or tenant in Unified CCDM.

4. If you select the **Customer Resource Mapping** option, complete the following information:

   a. Click ✚ to add a new customer resource mapping that defines the resource types and the specific resources of that type to be mapped to the selected import location.

   b. In the **Customer Resource Mapping** dialog box, select the resource type from the **Type** drop-down list (one of Peripheral, Routing Client, Media Routing Domain and Remote Tenant) then select the specific item of that type that you want to map from the **Resource** drop-down list.

   c. If you select the **Remote Tenant** option, you can optionally specify one of the following to use for the tenant mapping:

      - active directory settings, which enable you to associate a specific active directory with a tenant or folder.

      - small contact center settings, which enable you to configure a tenant or folder as a small contact center, create a department, and define department-level mappings.

      Note. A two way trust relationship is required between the customer domain and where the CCDM server is configured.

   d. If you want to specify active directory settings, select the **Active Directory Configuration** tab, and select **Configure Active Directory Settings**. Specify the domain controller and the authentication modes required, then click **Next**. Browse to the Active Directory folder you want to use, select it, and click **Update**.

      Note. The Active Directory settings for the remote tenant are updated immediately and will be retained even if you later exit ICE without saving your changes.

   e. If you want to configure a small contact center, select the **Small Contact Center Settings** tab and select **Enable Small Contact Center**. Enter the name of the department you want to create and click **Create Department**. The department will be created and provisioned, and any resources from the remote tenant that are associated with this department will be imported into the selected folder or tenant.

      Note. The specified department is provisioned and created immediately, and will be retained even if you later exit ICE without saving your changes. You cannot subsequently edit this department in ICE.

Note. Once a folder has been mapped as a small contact center folder, no other item mappings are allowed for this folder or any subfolders.

f.   When you have defined the customer resource mapping, click **OK**. Repeat these steps to add additional customer resource mappings if required.

Note

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

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

Note

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

5.   When you have finished defining the equipment mappings, click **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.

Replication

About Replication

About the Replication Manager

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

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

When your system is first installed you should:

•   configure replication as described in section "Configure Replication"

•   monitor replication as described in section "Monitor the Replication Snapshot"

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

About The Snapshot Process

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

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

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

About Replication Publications

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

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

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

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

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

Configure Replication

Note

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

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

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

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

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

   - **Database Name**. Enter the name of the Unified 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.

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

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

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

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

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

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

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

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

5.   The Identity Server should be replicated by default. To replicate the Identity Server Database, click the **Identity Database Replication Enabled** checkbox.

6.   If required, modify the distributor properties.

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

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

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

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

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

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

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

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

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

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

Monitor the Replication Snapshot

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

To monitor the progress of the replication snapshot:

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

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

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

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

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

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

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

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

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

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

   "Delivered snapshot from . . . "

   "No replicated transactions are available".

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

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

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

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

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

Unified CVP Media File Upload

About Unified CVP Media File Upload

Note

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

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

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

Prepare the Configuration

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

1. Make a note of the Host Name and IP Addresses of the Unified CVP media server or servers.

2. Make a note of the User Name and Password of a user with administrator rights on the domain so that you can configure DFS and File Replication.

3. Ensure that Microsoft DFS, File Replication and Remote Procedure Call services are installed and running on the Unified CVP media servers and the domain controller.

Configure Unified CVP Media File Upload - Windows Server 2003

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

Configure DFS for Unified CVP Media File Upload

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

1. Log in to the Domain Controller as a user with administrator rights.

2. Click **Start > Program Files > Administrative Tools > Distributed File System** to open the Distributed File System configuration utility.

3. Right-click on the Distributed File System node in the left of the screen and select **New Root** option to open the New Root Wizard.

4. Ensure that the option for **Domain Root** is selected in the **Root Type** window.

5. Follow the wizard by entering the default values. When you reach the **Host Server** window enter the Host Name of the Domain Controller.

6. For the Root Name field enter **PortalMedia** in the field provided.

7. For the **Folder to Share**, select the folder to contain the Unified CVP media files that are uploaded.

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

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

Configure DFS Root Targets

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

1. Right-click on the new root and select **New Root Target**.

2. Enter the server name for the Unified CVP media server.

3. For the **Folder to Share**, select the folder to contain the Unified CVP media files that are uploaded.

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

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

Configure File Replication for Unified CVP Media File Upload

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

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

To begin file replication:

1. Log in to the Domain Controller as an administrative user.

2. Click **Start > Program Files > Administrative Tools > Distributed File System** to open the Distributed File System configuration utility.

3. Right-click 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.

Configure Unified CVP Media File Upload - Windows Server 2008

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

Create a Shared Namespace

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

1. Log in to the Domain Controller as a user with administrator rights.

2. Click **Start > Program Files > Administrative Tools > Server Manager** to open the Server Manager utility.

3. In Server Manager, expand the **Roles** node, the **File Services** node, and the **DFS Management** node to see the Namespaces node. Right click on **Namespaces**, and select **New Namespace** to run the New Namespace Wizard.

4. In the Namespace Server window, enter the name of the primary Unified CCDM Database Server and click **Next**.

5. In the Namespace Name and Settings window, enter **PortalMedia** for the namespace name.

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

6. Click **Edit Settings**, review the shared folder permissions, and change them as required, if necessary. Click **OK**, then click **Next**.

7. In the Namespace Type window, select **Domain-based namespace** and click **Next**.

8. Review the namespace settings, and click **Create** to create the namespace you have specified. When the namespace has been created, click **Close**.

Configure Replication

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

1.   On the domain controller, in the Server Manager utility, expand the **Roles** node, the **File Services** node, and the **DFS Management** node to see the Replication node. Right click on **Replication**, and select **New Replication Group** to run the New Replication Group Wizard.

2.   In the Replication Group Type window, select **Multipurpose replication group**, and click **Next**.

3.   In the Name and Domain window, enter a name for the replication group, for example, **sharePortalMedia**. Click **Next**.

4.   In the Replication Group Members window, click **Add**, and in the Select Computers window, enter the name of one of the CVP media servers to be included in the replication group. Click **OK** to add the specified server to the replication group.

5.   Repeat the step above to add each of the remaining CVP media servers to the replication group.

6.   Click **Next**.

7.   In the Topology Selection Window, select **Full mesh** and click **Next**.

8.   In the Replication Group Schedule and Bandwidth window, select **Replicate continuously using the specified bandwidth** and click **Next**.

9.   In the Primary Member window, choose one of the CVP media servers in the replication group to be the **Primary member**, and click **Next**.

10.   In the Folders to Replicate window, click **Add**, then **Browse**. Select the folder on the primary server where the CVP media files are stored and click **OK**.

11.   In the Local path on Other Members window, select one of the other CVP media servers in the replication group and click **Edit**.

12.   In the Edit window, select **Enabled**, then **Browse**, and locate the folder on this server where the CVP media files are stored. Click **OK**.

13.   Repeat the previous two steps for any other CVP media servers in the list of servers. Click **Next**.

14.   Review the replication settings, and click **Create** to set up the replication you have specified. When the replication has been set up, click **Close**.

Share and Publish the Replicated Folder

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

1.   On the domain controller, in the Server Manager utility, expand the **Roles** node, the **File Services** node, and the **DFS Management** node to see the Replication node. Click on the replication group you created above, and select the **Replicated Folders** tab.

2.   In the Publishing Method window, select **Share and Publish the Replicated Folder in a Namespace** and click **Next**.

3. In the Share Replicated Folders window, select one of the CVP media servers in the replication members section, and click **Edit**. Review the shared folder permissions, and change them as required, if necessary. Click **OK.**

4. Repeat the step above to set the folder permissions for each of the remaining CVP media servers in the replication group. Click **Next** when you have finished.

5. To set Parent folder in namespace, in the Namespace Path window click **Browse**, select **\\<domain>\PortalMedia** from the list (this is the namespace you created above), and click **OK**.

6. In the Namespace Path window, enter the New folder name as **CVP**. Click **Next**.

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

Configure the Replicated Folder for Media File Upload

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

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

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

   - **Database Name**. Enter the name of the Unified 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.

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

3. In the **Tools** drop-down, select **System Properties Manager** and on the **Global** tab, navigate to the **Media Upload** group.

4. Change the Media Share property from the default value of **PortalMedia** to **PortalMedia\CVP**.

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

6. Close ICE.

Test the CVP Upload Configuration

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

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

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

Post-Installation Steps

About Post-Installation Steps

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

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

Configure SSL

About Configuring SSL for Unified CCDM

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

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

To configure SSL for Unified CCDM you need to:

- obtain a digital certificate if you do not already have a suitable one (see section "Obtain a Digital Certificate")
- export the certificate in PFX format (see section "Export the Certificate in PFX Format")
- configure SSL for the Unified CCDM web application (see section "Configure SSL for the Web Application").

Obtain a Digital Certificate

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

- purchased from an external certificate authority, for public use

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

> **Note**
>
> We recommend a digital certificate with a key length of at least 2048 bits. Some recent browsers may reject certificates with shorted key lengths.

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

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

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

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

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

  - To *request an external certificate*:

    - In the **Actions** pane, select **Create Certificate Request** to display the **Request Certificate** dialog box.
    - In the **Common Name** field, enter the application domain name as defined above.
    - Complete the other fields as appropriate, and click **Next**.
    - In the **Cryptographic Service Provider Properties** dialog box leave the default **Cryptographic Service Provider**. Select a bit length of at least 2048. Click **Next**.
    - Specify a file name for the certificate, and then click **Finish**.
    - When you receive the certificate from the certificate authority, repeat step 1. and step 2. above to show the Server Certificates and Action panes, and in the **Action** pane, select **Complete Certificate Request.**
    - Enter the file name of the certificate, and a Friendly Name of your choice and click **OK**.

- To *generate an internal certificate*:

  - Select **Create Domain Certificate** in the **Actions** pane to display the **Distinguished Name Properties** dialog box.

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

  - Complete the other fields as appropriate, and click **Next**.

  - In the **Online Certification Authority** dialog box specify the **Online Authority** and **a Friendly Name**. Click **Finish.**

Export the Certificate in PFX Format

To export the certificate in PFX format:

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

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

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

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

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

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

Configure SSL for the Web Application

To configure SSL for the web application:

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

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

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

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

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

   SSL Configuration Complete.

Bind Server Ports to IPv6 Addresses

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

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

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

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

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

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

Configure Antivirus Options

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

*   The folders containing the database files (***.ldf**, ***.mdf** and ***.ndf**) on the Database Server. To locate these files, start **SQL Management Studio**, expand the **Databases** node, and select **Properties** for the database. If you selected the default database name at installation, the database will be **Portal**. In the Database Properties dialog box, select the **Files** page to see the folder and file names of the database files.

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

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

Performance Tuning Checklists

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

App/Web Servers

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

Database Servers

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

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

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

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

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

Final Post-Installation Actions

Restart the System

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

Log in to Unified CCDM

Launch the **Domain Manager** application. This will open a web page, which you can bookmark.

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

Note

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

Verify the Installation

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

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

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

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

```
Select count(*)
from [dbo].[TB_DIM_AGENT]
```

This query should return a value of at least 3.

Single-Sided Upgrade

About a Single-Sided Upgrade

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

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

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

Checklist for Single-Sided Upgrades

Step	Complete
section "Prepare to Upgrade"	
Stop the Unified CCDM Services	
Back up the Unified CCDM portal database	
Configure new windows servers	
Create user accounts	
Apply optional security configuration	
section "Install SQL Server and Restore Database"	
Install and configure SQL Server	
Restore the portal database	
Add network service accounts	
section "Upgrade and Configure Unified CCDM Components"	
Install the Database Components	
Upgrade the portal database	

Step	Complete
Install the App/Web Server	
Reconfigure the Unified CCDM servers	
Reconfigure the Unified CCE Servers	
Reconfigure Unified CCE to use new servers	
Post-Upgrade actions	
section "Restart and Validate"	
Restart the Unified CCDM services	
Validate the upgrade	

Prepare to Upgrade

Stop the Unified CCDM Services

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

Stop the Unified CCDM Database Server Services

On the Database Server:

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

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

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

Stop the Unified CCDM App/Web Server Services

On the App/Web Server:

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

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

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

Back up the Portal Database

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

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

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

2.   Navigate to the Portal database.

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

4.   Close SQL Server Management Studio.

Configure New Windows Servers

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

Create User Accounts

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

Apply Optional Security Configuration

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

Uninstall Unified CCDM Components

Uninstall Unified CCDM Components as described in section "About Uninstalling Unified CCDM".

Install SQL Server and Restore Database

Install and Configure SQL Server

On the Database Server:

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

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

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

Restore the Portal Database

Restore the portal database from the backup you made earlier.

On the Database Server:

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

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

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

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

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

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

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

Add Network Service Accounts

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

On the Database Server:

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

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

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

> **Note**
>
> Do not delete the entry for the NETWORK SERVICE account for the local machine (**NT AUTHORITY\NETWORK SERVICE**).
>
> The NETWORK SERVICE logins for remote web server machines in the deployment are of the form **<DOMAIN>\<WEBSERVER MACHINE NAME>$**. For example, if your web server is called **WEBSERVERA** and belongs to the **UCCDMDOM** domain, the NETWORK SERVICE login would be **UCCDM\WEBSERVERA$**.

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

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

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

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

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

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

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

11. Click **OK**.

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

Upgrade and Configure Unified CCDM Components

The previous Unified CCDM components need to be uninstalled prior to the installation of upgraded components.

Install the Database Components

On the Database Server:

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

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

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

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

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

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

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

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

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

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

   > **Warning!**
   > You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you continue the installation with a new passphrase you will be unable to access your existing data.

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

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

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

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

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

- Click **Next**.

9. In the **Destination Folder** window, if you want to change the location where the database components are stored, click **Change** and select the new location. The Unified CCDM components need to be installed in the same directory location on each of the servers.

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

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

12. Click **Finish**.

Upgrade the Portal Database

On the Database Server:

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

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

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

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

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

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

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

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

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

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

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

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

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

Install the App/Web Server

On the App/Web Server:

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

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

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

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

5. If the **Domain Manager: Application Server Components** dialog is displayed, click **Install** to install the additional required components.

6. If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.6 Framework is complete, restart the server to continue the installation of the App/Web Server.

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

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

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

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

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

- Click **Next** to continue.

> **Warning!**
>
> You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you continue the installation with a new passphrase you will be unable to access your existing data.

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

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

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

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

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

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

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

- Click **Next** to continue.

11. Click **Install**.

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

Reconfigure the Unified CCDM Servers

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

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

To update the cluster configuration, on the Database Server:

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

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

    *   **Database Name**. Enter the name of the Unified 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.

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

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

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

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

    *   **Primary Server**

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

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

    *   **Secondary Server**:

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

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

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

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

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

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

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

Reconfigure the Unified CCE Servers

> **Note**
>
> This step is only required if you have upgraded Unified CCE at the same time as upgrading Unified CCDM. This step is not required if you have not upgraded Unified CCE.

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

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

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

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

    • **Database Name**. Enter the name of the Unified 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.

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

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

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

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

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

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

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

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

- **Local Registry Port**. This is the port on the Unified CCE for the Unified 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.

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

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

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

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

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

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

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

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

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

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

Reconfigure Unified CCE to Use the New Servers

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

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

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

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

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

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

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

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

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

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

Post-Upgrade Actions

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

*   configure HTTPS as described in section "Configure SSL"

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

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

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

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

Note

If your installation uses single sign-on, the configuration is restored when the database is restored, so you do not need to reconfigure single sign-on as described in section "Configure Windows Login"

Restart and Validate

Restart the Unified CCDM Services

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

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

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

2. For each Unified CCDM service listed:

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

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

Note

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

Validate the Upgrade

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

Upgrading From a Previous Version

About the Upgrade Procedure

General Information

Notes

Before proceeding with the upgrade, previous Unified CCDM components must be uninstalled.

This version of Unified CCDM requires Windows Server 2012 R2 and SQL Server 2014 SP2. Earlier versions of Unified CCDM used Windows Server 2008 and SQL Server 2008. Before upgrading from Unified CCDM 10.0(1) or earlier, the servers must be completely rebuilt. In-situ upgrades are not supported. You can either prepare new servers running Windows Server 2012, or you can rebuild your existing servers.

Upgrade Options

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

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

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

More About Upgrading Dual-Sided Systems

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

Failover information for the individual Unified CCDM components is stored in the databases on Side A and B. This information is also replicated using SQL Server replication. This means that both sides have knowledge of the primary and secondary server configuration made through the Unified CCDM Integrated Configuration Management tool, even when replication has been removed.
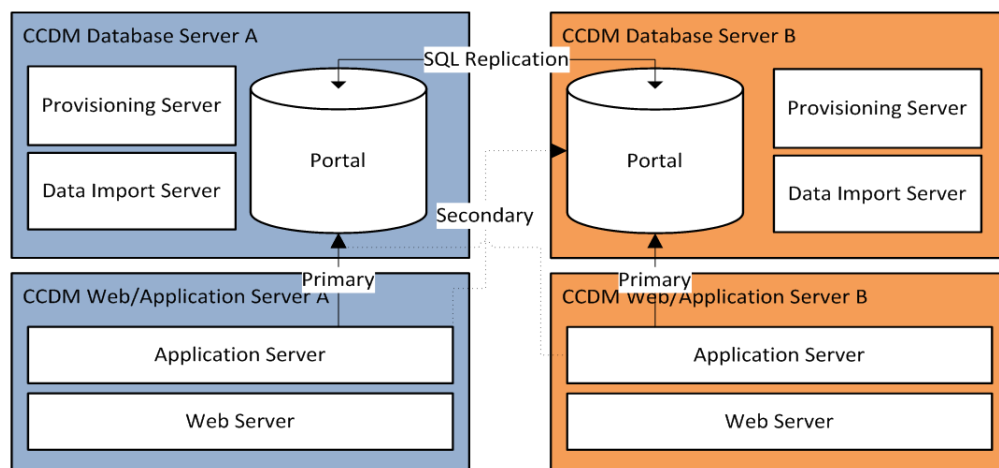
Figure 8.1   Replication and Failover Connections

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

There are two ways to upgrade dual-sided systems:

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

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

Identity Server

The Identity Server is now a required component. You will have to follow the installation steps of Identity Server from the Product Installation section of this guide. The Identity server should be installed after installing the Web/App component. For rest of the components you can refer to the upgrade section as usual.

Once the Upgrade has finished

After the database has been upgraded, the Setup UCCMP Servers Wizard must be run to set the FQDN to access the web site.

User Migration Tool

You can access the User Migration Tool from the Unified CCDM CD Drive, by opening the **SSO** folder, and then the **MigrateUsers** folder.

The User Migration Tool can be run post upgrade on the application server. It converts old users settings by updating ISE users to local users. Their username must match the unique principal name of the Active Directory user, for example "user@domain.local". The password must be set and marked as "must change at next login". The user must set the password to be the same as the Active Directory password on login. Any other users that are using SSO need to have their login name set to "DOMAIN\user".

On running the tool, there are the following options:

- **SSO**: Whether the system was in SSO mode before upgrade.

- **Authentication Types**: The type of authentication you want the tool to look for. The tool will look for ISE users by default. Set to True to look for all authentication types.

- **ActiveDirectoryPath**: The Active Directory path. If left empty, the tool will attempt to bind to the global catalog of the domain the application server is connected to with default settings.

- **UserPassword**: The password you want to set local users to use, mark as "must change at next login".

- **HashingAlgorithm**: The hashing algorithm that the system uses to hash passwords. Set to "SHA256Salt = 6" by default.

- **DeleteUsersThatFailToMigrate**: Select to delete local users that have a "NULL" password or Active Directory users with the wrong name format. Default is set to false. All deleted users can be restored if necessary.

Once the tool has been run, a log file is generated. The log file displays the User IDs of all the users that have been updated, and for all that have failed.

The tool can be run as many times as necessary.

Validating an Upgrade

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

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

Total Outage Upgrade

About a Total Outage Upgrade

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

Warning!

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

Note

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

Checklist for Total Outage Upgrades

Step	Complete
section "Prepare to Upgrade"	
Stop the Unified CCDM services	
Remove database replication	
Backup the Unified CCDM portal databases	
Configure new windows servers	
Create user accounts	
Apply optional security configuration	
section "Install SQL Server and Restore the Database"	
Install and configure SQL Server	
Restore the portal database	
Configure the SQL Agent user	

Step	Complete
Add network service accounts	
section "Install and Configure SQL Server "	
Install the Database Components	
Upgrade the portal database	
Install Database Components and Upgrade portal database (Side B)	
Install the App/Web Server	
Reconfigure the Unified CCDM servers	
Reconfigure the Unified CCE Servers	
Reconfigure Unified CCE to use new servers	
section "Restore Replication"	
Configure Replication	
Monitor the replication snapshot	
Post-upgrade actions	
section "Restart and Validate"	
Restart the Unified CCDM services	
Validate the upgrade	

Prepare to Upgrade

Stop the Unified CCDM Services

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

Stop the Unified CCDM Database Server Services

On the Side A Database Server:

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

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

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

Repeat these steps on the Side B Database Server.

Stop the Unified CCDM App/Web Server Services

On the Side A App/Web Server:

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

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

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

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

Remove Database Replication

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

To remove database replication:

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

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

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

   - **Database Name**. Enter the name of the Unified 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**. The ICE Cluster Configuration tool starts by default.

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

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

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

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

Back up the Portal Database

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

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

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

2.   Navigate to the Portal database.

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

4.   Close SQL Server Management Studio.

Repeat these steps on the Side B Database Server.

Configure New Windows Servers

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

Create User Accounts

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

Apply Optional Security Configuration

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

Uninstall Unified CCDM Components

Uninstall Unified CCDM Components as described in section "About Uninstalling Unified CCDM".

Install SQL Server and Restore the Database

Install and Configure SQL Server

On the Side A Database Server:

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

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

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

Repeat these steps on the Side B Database Server.

Restore the Portal Database

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

On the Side A Database Server:

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

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

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

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

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

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

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

Repeat the process on the Side B Database Server to restore the Side B portal database backup to the Side B Database Server.

Configure the SQL Agent User

For a dual-sided system, the SQL Agent User must be reconfigured.

On the Side A Database Server:

1. Launch **SQL Server Management Studio** and expand the **Security** folder. A list of subfolders is displayed.

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

3. Ensure the **Windows authentication** option is selected and enter the SQL Agent User domain and login name in the form **<DOMAIN>\<LOGIN>**. This should be the user name that you specified for the SQL agent user account when you originally installed the portal database. For example, if your user is called **sql_agent_user** and belongs to the **CISCO** domain, enter **CISCO\sql_agent_user.**

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

5. In the **Users mapped to this login** section, select the **Portal** database. The User column will auto-populate with the domain user name for the SQL Agent User.

6. In the **Database Role Membership** section, select the **db_owner** role.

7. Click **OK** to apply the changes.

Repeat these steps on the Side B Database Server.

Add Network Service Accounts

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

On the Side A Database Server:

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

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

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

> **Note**
>
> Do not delete the entry for the NETWORK SERVICE account for the local machine (**NT AUTHORITY\NETWORK SERVICE**).
>
> The NETWORK SERVICE logins for remote web server machines in the deployment are of the form **<DOMAIN>\<WEBSERVER MACHINE NAME>$**. For example, if your web server is called **WEBSERVERA** and belongs to the **UCCDMDOM** domain, the NETWORK SERVICE login would be **UCCDM\WEBSERVERA$**.

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

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

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

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

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

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

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

11. Click **OK**.

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

Repeat these steps on the Side B Database Server.

Configure Replication Share

For a dual-sided system, the replication share folder must be reconfigured.

On the Side B Database Server:

1. In the SQL Server installation folder, locate the replication folder. Typically this is located at **C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\repldata**.

2. Create a share for this folder, giving the **Everyone** group full control to the share, as follows:

    a. Right-click on the replication folder and select **Share With > Advanced sharing**.

    b. On the **Sharing** tab, click **Advanced Sharing**.

    c. Select **Share this folder** and specify the share name as the name that was used for the replication folder when you originally installed the portal database. The default name is **ReplData**.

    d. Click **Permissions**, select the group **Everyone**, and allow all permissions.

3. Click **OK** to apply the changes.

Upgrade and Configure Unified CCDM Components

Install the Database Components

On the Side A Database Server:

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

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

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

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

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

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

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

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

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

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

> **Warning!**
> You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you continue the installation with a new passphrase you will be unable to access your existing data.

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

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

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

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

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

   - Click **Next**.

9. In the **Destination Folder** window, if you want to change the location where the database components are stored, click **Change** and select the new location. The Unified CCDM components need to be installed in the same directory location on each of the servers.

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

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

12. Click **Finish**.

Upgrade the Portal Database

On the Side A Database Server:

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

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

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

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

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

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

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

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

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

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

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

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

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

Install Database Components and Upgrade Portal Database (Side B)

On the Side B Database Server:

1.   Install the database components as described in section "Install the Database Components".

2.   Upgrade the Portal database as described in section "Upgrade the Portal Database".

Install the App/Web Server

On the Side A App/Web Server:

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

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

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

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

5.   If the **Domain Manager: Application Server Components** dialog is displayed, click **Install** to install the additional required components.

6.   If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.6 Framework is complete, restart the server to continue the installation of the App/Web Server.

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

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

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

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

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

   • Click **Next** to continue.

> **Warning!**
> You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you continue the installation with a new passphrase you will be unable to access your existing data.

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

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

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

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

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

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

11. Click **Install**.

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

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

Reconfigure the Unified CCDM Servers

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

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

This only needs to be done on the Side A Database Server. The Side B servers will be updated when replication is reinstated. To update the cluster configuration, on the Side A Database Server:

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

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

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

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

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

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

*   **Primary Server**

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

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

*   **Secondary Server**:

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

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

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

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

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

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

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

These steps do not need to be repeated on the Side B Database Server as the necessary changes will be applied when replication is reinstated.

Reconfigure the Unified CCE Servers

Note

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

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

This only needs to be done on Side A. Side B will be updated when replication is reinstated. To reconfigure the Unified CCE servers after Unified CCE has been upgraded, on the Side A Database Server:

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

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

    *   **Database Name**. Enter the name of the Unified 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.

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

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

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

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

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

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

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

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

    *   **Local Registry Port**. This is the port on the Unified CCE for the Unified 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.

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

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

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

8.   On the **Multi Media Support** page, if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance to provide support for non-voice interactions, select **Yes**. The default is No.

9.   On the **Purge On Delete** page, if you want to purge items from Unified CCE automatically when they are deleted from Unified CCDM, select **Yes**. The default is Yes.

10. On the **Supervisor Active Directory Integration** page, if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors, select **Yes**. The default is No. If you select Yes, you will be prompted to provide Active Directory information so that Windows user accounts can be listed.

11. The Summary dialog box summarizes the details of the Unified CCE being configured and the settings you have chosen. Check the details, and if you are satisfied, click **Next**.

12. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.

13. For each remaining Unified CCE Server that has been upgraded, click **Configure Cisco Unified CCE Servers**, and repeat the steps above.

14. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu.

These steps do not need to be repeated on the Side B Database Server as the necessary changes will be applied when replication is reinstated.

Reconfigure Unified CCE to Use the New Servers

Note

This step is only required if you have reinstalled Unified CCDM on new servers with different names. This step is not required if you have upgraded your existing servers, or have replaced your existing servers with new servers with the same names.

If you have reinstalled Unified CCDM on new servers with different names, Unified CCE must be updated to reference the new Unified CCDM servers.

To do this, on each Unified CCE instance in your Side A deployment:

1.   Launch **CMS Control**. This opens the CMS control console.

2.   On the **Application** tab, select the Unified CCDM database server and click **Edit**.

3.   In the **Application connection details** tab, change the existing server name to the new server name. There are three places where this needs to be done:

     • **Administration & Data Server Link**. The name of the newUnified CCDM Database Server, in capital letters, with **Server** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBServer**.

- **Application link**. The name of the new Unified CCDM Database Server, in capital letters, with **Client** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBClient**.

- **Application host name**. The name of the new Unified CCDM Database Server, in capital letters, for example, **PRODUCTDB**.

4. **Click** OK, then **OK** again to save the changes and exit CMS Control.

Repeat these steps on each Unified CCE instance in your Side B deployment.

Restore Replication

Configure Replication

Replication between the databases is set up and monitored using the Replication Manager application which is available in the Unified CCDM Integrated Configuration Environment (ICE) tool.

> **Note**
>
> The user running Replication Manager must have administrator permissions in both Windows and SQL Server, for both the publisher and the subscriber Database Servers.
>
> Usually, the publisher will be the Side A Database Server, but occasionally, it may be necessary to configure the Side B Database Server as the publisher.

To configure replication, on the publisher Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCDM). In the **Database Connection** dialog box, set:

   - **Server Name**. Enter the name of the primary database server.

   - **Database Name**. Enter the name of the Unified 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.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. From the Tool drop-down list, select **Replication Manager**. The Replication Manager opens in the Setup tab. The Setup tab has the following sections:

   - **Unified CCDM Database Server Properties** contains the publisher and subscriber Unified CCDM database details.

   - **Distributor Properties** contains the SQL Server Replication distributor properties.

The default values shown in the Setup tab are derived from the values initially configured in the Cluster Configuration tool and will be suitable in most cases.

4. If required, modify the Unified CCDM Database Server Properties.

    - **Server Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.

    - **Catalog Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration. It may be changed, but if so, a valid database with the new name must already exist on the corresponding server.

5. The Identity Server should be replicated by default. To replicate the Identity Server Database, click the **Identity Database Replication Enabled** checkbox.

6. If required, modify the distributor properties.

    - **Server Name**. The name of the subscriber server hosting the Unified CCDM database. This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.

    - **Catalog Name**. The name to be assigned to the distribution database. The recommended value is **distribution_portal**.

    - **Data Folder**. The folder path on the distributor server where the data file for the distribution database will be created.

    > **Note**
    >
    > If you are setting up replication after performing an upgrade, be particularly careful with the Data Folder path, as it may be different from the value used in previous versions of Unified CCDM. Make sure you use the path that was specified when the database was set up.

    - **Log Folder**. The folder path on the distributor server where the transaction log file for the distribution database will be created.

    - **Distribution Share**. The distribution share folder where replication snapshot files will be generated.

    - **Override Distributor Admin Password**. Select to override the auto-generated replication password which will be used to establish connectivity. The auto-generated password is 14 characters long, and will contain alpha-numeric characters (both upper and lower case) and a special character. If this does not meet the complexity requirements of the server then select this option and specify a password of your choice.

7. When you have set the required replication properties, click **Configure** to configure replication.

8.   You may be prompted to save pending changes to the database before continuing. If so, click **Yes** to save pending changes and continue.

9.   It may take several minutes to configure replication. Once replication has been configured, the Replication Manager automatically switches to the Monitor tab, which enables you to monitor the progress of the replication snapshot.

Monitor the Replication Snapshot

> **Note**
>
> The subscriber Database Server is not available for use until the replication snapshot has completed and all the data has been copied from the publisher to the subscriber.
>
> The time taken for the replication snapshot to complete depends on the volume of data in the publisher database and the bandwidth between the servers. For a large database, this may take several hours.

To monitor the progress of the replication snapshot:

1.   In the ICE Replication Manager, select the **Monitor** tab. The Monitor tab has the following panes:

   •   **Publications** (top left) lists the publisher servers and the publications on each publisher that need to be shared with the subscribers.

   •   **Subscriptions and Agents** (top right) shows the subscriptions to a publication and the replication agents associated with a publication. This pane has two tabs, Subscriptions and Agents.

   •   **Subscriptions** shows the subscriptions to the selected publication. You can right-click on a subscription to start or stop the subscription.

   •   **Agents** shows the replication agents associated with the selected publication. You can right-click on a replication agent to start or stop the agent.

   •   **Sessions** (bottom left) shows all sessions for the selected publication and replication agent in the last 24 hours.

   •   **Actions** (bottom right) shows the activity for the selected session.

2.   In the top left hand pane, select the first Unified CCDM database publication from the list of publications. If you have used the default database name, this will start with **[Portal]**.

3.   Wait for the replication snapshot for this publication to complete.

   To check the replication status for a Unified CCDM database publication, in the bottom right hand pane of the Monitor tab, inspect the messages in the Action Message list. Once the replication snapshot is complete and replication is operational for a publication, you will see the following two messages:

   "Delivered snapshot from . . . "

"No replicated transactions are available".

After this, the second message is replaced with messages showing new replicated transactions as they are sent through the system, for example:

"4 transaction(s) with 14 command(s) were delivered".

4.   Repeat the two steps above for each of the remaining Unified CCDM database publications.

5.   When replication is complete for all portal database publications, close the ICE tool.

The subscriber database can now be used to service requests. For more information about the Replication Manager see the *Integrated Configuration Environment (ICE) for Cisco Unified Contact Center Domain Manager*.

Post-Upgrade Actions

After you have upgraded Unified CCDM, complete the following post-installation steps:

- configure HTTPS as described in section "Configure SSL"
- bind server ports to IPv6 addresses as described in section section "Bind Server Ports to IPv6 Addresses"
- configure anti-virus operations as described in section "Configure Antivirus Options"
- implement the performance tuning steps described in section " Performance Tuning Checklists"
- complete the final post-installation actions described in section "Final Post-Installation Actions"

Note

If your installation uses single sign-on, the configuration is restored when the database is restored, so you do not need to reconfigure single sign-on as described in section "Configure Windows Login"

Restart and Validate

Restart the Unified CCDM Services

Following an upgrade it is good practice to restart all Unified CCDM services.

Repeat the following steps on each upgraded Unified CCDM Database Server and each and upgraded Unified CCDM App/Web Server:

1.   In the **Run** command dialog box, enter **Services.msc** and click **OK**.

2.   For each Unified CCDM service listed:

*   if the selected service is in the Started state, right-click the service name and click **Restart**

*   if the selected service is not started, right-click the service name and click **Start**.

Note

After starting the System Monitoring Service and Application Service on the App/Web Server, you will need to wait a few minutes before logging in to allow the services to load completely.

Validate the Upgrade

Check that the system is functional following the upgrade using the validation tests in section "Validating an Upgrade".

Split Sided Upgrade

About a Split Sided Upgrade

This chapter describes the steps involved to upgrade a dual-sided deployment, where the system is split, and one side is upgraded at a time. Until the second side is upgraded, you will be running two different versions of Unified CCDM side by side.

This upgrade process temporarily breaks the replication and communication channels between the two sides of the system so each side can operate independently as a single-sided system. When replication is restored, the configuration from Side A of the system will replace all configuration on Side B of the system.

> **Note**
>
> Use this mode of operation with caution. Unified CCE and Unified Communications Manager changes committed to Side B will be imported from the AW onto Side A, but any Unified CCDM specific configuration items (for example folders, users, security etc.) that are added, changed or deleted on Side B after the system was split will not be reflected on Side A, even after side B is upgraded and replication is restored.

This process has two parts.

- Part 1 - split the dual-sided system and upgrade Side A (see section "Checklist for Split Side Upgrades (Side A)").

- Part 2 - upgrade Side B and restore replication (see section "Checklist for Split Side Upgrades (Side B)").

There are two options for restoring the Side B database. They are:

- **Option 1**. Restore the Side B database from the Side B backup taken before the upgrade, then upgrade the restored database. This is the recommended method if the system has been running in single-sided mode for less than 24 hours.

- **Option 2**. Restore the Side B database from the upgraded Side A database. In this case, you will not need to upgrade the database after you have restored it. This is the recommended method if the system has been running in single-sided mode for more than 24 hours.

The description assumes that you have a two tier deployment (separate database and app/web servers) although you can still use these instructions if you have an all-in-one installation.

> **Warning!**
>
> Ensure that you have up-to-date backups of all Unified CCDM databases before you begin the upgrade. Instructions for doing this are included here.

> **Note**
>
> Before starting the upgrade please ensure you have the original cryptographic passphrase from the original Unified CCDM installation as you will need it during the upgrade.

Checklist for Split Side Upgrades (Side A)

The first part of the split side upgrade splits the dual-sided system and upgrades Side A.

Step	Complete
section "Prepare to Upgrade (Side A)"	
Stop the Unified CCDM services	
Force failover connections to the Active Side	
Update Side B to enable provisioning and import (optional)	
Remove database replication	
Backup the Portal Database	
Configure new windows servers	
Create user accounts	
Apply optional security configuration	
section "Install SQL Server and Restore the Portal Database (Side A)"	
Install and configure SQL Server (Side A)	
Restore the portal database (Side A)	
Configure the SQL Agent user (Side A)	
Add network service accounts (Side A)	
section "Upgrade and Configure Unified CCDM Components - Side A"	
Install the Database Components	
Upgrade the portal database	
Install the App/Web Server	
Reconfigure the Unified CCDM servers	
Reconfigure the Unified CCE Servers	

Step	Complete
Reconfigure Unified CCE to use new servers	
Post-upgrade actions	
section "Restart and Validate (Side A)"	
Restart the Unified CCDM services	
Validate the upgrade	

Prepare to Upgrade (Side A)

Stop the Unified CCDM Services

Before starting the upgrade, you must stop all Unified CCDM services on all servers.

Stop the Unified CCDM Database Server Services

On the Side A Database Server:

1. In **services.msc**, stop the **UCCDM: Data Import Server** service.
2. Repeat this step for the UCCDM**: Partitioning Table Manager** service.
3. Repeat this step for the UCCDM**: Provisioning Server** service.

Stop the Unified CCDM App/Web Server Services

On the Side A App/Web Server:

1. In **services.msc**, stop the **UCCDM: System Monitoring Services** service.
2. If you see a prompt saying that all other services will stop, and asking you if you want to continue, select **Yes**.
3. If there are any other running Unified CCDM services, stop them too.

Force Failover Connections to the Active Side

To operate the two sides as independent systems, add host file entries to point failover connections to the current active side. This reduces the possibility that a failover will occur to the database on the other side when replication is down.

Since the failover information is held in the database, both sides know about the other side, even though they are currently not replicated or running the same version of Unified CCDM. If a failover occurs then data integrity will be lost. To avoid this, when operating in single-sided mode add the failover connections to the hosts file on each machine to point back to the active side.

For example, in the deployment shown in Figure 10.1 "Host File Entries For Failover in Single-sided Mode", the host file entries are:

DBA

```
127.0.0.1                 DBB
```

DBB

```
127.0.0.1                 DBA
```

WEBA

```
<IP ADDRESS OF DBA>       DBB
127.0.0. 1                WEBB
```

WEBB

```
<IP ADDRESS OF DBB>       DBA
 127.0.0. 1               WEBA
```
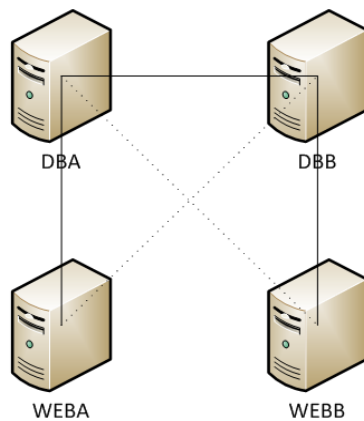

Figure 10.1   Host File Entries For Failover in Single-sided Mode

These entries must be removed once the upgrade is complete and replication between Side A and Side B is restored.

Update Side B to Enable Provisioning and Import (Optional)

If the sides of the system are to be run independently for some time, you may need to enable provisioning and import to run on both Side A and Side B at the same time.

To do this, follow the "Manual Provisioning/Import Failover" steps described in the *Administration Guide for Cisco Unified Contact Center Domain Manager* for the version of Unified CCDM that is currently running on the Side B Database Server.

Remove Database Replication

Before you can upgrade a dual-sided system, database replication must be removed.

To remove database replication:

1.   Ensure you are logged in to the Side A Database Server as a domain level user with administrative rights over both Database Servers.

2.   Launch **Integrated Configuration Environment** (installed as part of Unified CCDM). In the **Database Connection** dialog box, set:

      •   **Server Name**. Enter the name of the primary database server.

      •   **Database Name**. Enter the name of the Unified 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**. The ICE Cluster Configuration tool starts by default.

4.   From the Tool drop-down list select **Replication Manager**.

5.   Click the **Setup** tab to see the replication setup details.

6.   Click **Disable** to remove replication from the Unified CCDM database. When prompted, click **Yes** to proceed with replication removal.

7.   Replication removal may take several minutes. Wait for the 'Replication Removed' message to display in the Output Window and then exit ICE.

Back up the Portal Database

Back up the Portal database and copy the backup to a safe location where it can be accessed once the latest version of Unified CCDM has been installed on the new servers.

To back up the Portal database, on the Side A Database Server:

1.   Launch **SQL Server Management Studio**.

2.   Navigate to the Portal database.

3.   Right-click **Portal** and select **Tasks > Backup**. Save the **.bak** file to a suitable location.

4.   Close SQL Server Management Studio.

Configure New Windows Servers

On the new Side A servers running Windows Server 2012 R2, apply the Windows post-installation configuration in section "Windows Configuration".

Create User Accounts

Create the SQL Agent User account as described in section "User Accounts"

Apply Optional Security Configuration

On the new Side A servers running Windows Server 2012 R2, apply the security settings described in section "Optional Security Configuration"

Uninstall Unified CCDM Components

Uninstall Unified CCDM Components as described in section "About Uninstalling Unified CCDM".

Install SQL Server and Restore the Portal Database (Side A)

Install and Configure SQL Server (Side A)

On the Side A Database Server:

1. Install SQL Server 2014 as described in section "Install SQL Server".

2. Configure the SQL Server network protocols as described in section "Configure SQL Server Network Protocols".

3. Configure the Windows Firewall for SQL Server as described in section "Configure Windows Firewall for SQL Server".

Restore the Portal Database (Side A)

Restore the Side A portal database from the Side A backup you made earlier.

On the Side A Database Server:

1. Launch **SQL Server Management Studio**.

2. Right-click the **Databases** folder and click **Restore Database**.

3. In the Restore Database window choose **From Device**, click **Add** and add the location of the database back up file you want to restore from. You may need to copy the backup file to a local file in order to access it. Click **OK**.

4. Select the check box next to the backup set you just added.

5. From the **To Database** drop-down list, select the **Portal** database as the restore destination.

6. Select **Options** and choose **Overwrite the existing database**. This will restore the database to the same location as the previous database. If you would like to choose a different location, update the **Restore As** path for each file to your preferred data file location.

7. Click **OK** to start the restore.

Configure the SQL Agent User (Side A)

For a dual-sided system, the SQL Agent User must be reconfigured.

On the Side A Database Server:

1. Launch **SQL Server Management Studio** and expand the **Security** folder. A list of subfolders is displayed.

2. Right-click the **Logins** folder and select **New Login**.

3. Ensure the **Windows authentication** option is selected and enter the SQL Agent User domain and login name in the form **<DOMAIN>\<LOGIN>**. This should be the user name that you specified for the SQL agent user account when you originally installed the portal database. For example, if your user is called **sql_agent_user** and belongs to the **CISCO** domain, enter **CISCO\sql_agent_user.**

4. In the **Select a page** pane on the left hand side, click **User Mapping**.

5. In the **Users mapped to this login** section, select the **Portal** database. The User column will auto-populate with the domain user name for the SQL Agent User.

6. In the **Database Role Membership** section, select the **db_owner** role.

7. Click **OK** to apply the changes.

Add Network Service Accounts (Side A)

You must add the NETWORK SERVICE account for all web servers to the database logins with appropriate access permissions. Before this can be done the existing accounts must be deleted from the Portal database logins.

On the Side A Database Server:

1. Launch **SQL Server Management Studio** and in the Object Explorer, expand the **Portal** database. A list of folders is displayed.

2. Expand the **Portal > Security > Users** folder. A list of database logins is displayed.

3. For each occurrence of the **NETWORK SERVICE** account for a remote web server in the deployment, right-click it and select **Delete**.

> **Note**
>
> Do not delete the entry for the NETWORK SERVICE account for the local machine
> (**NT AUTHORITY\NETWORK SERVICE**).
>
> The NETWORK SERVICE logins for remote web server machines in the deployment are
> of the form **<DOMAIN>\<WEBSERVER MACHINE NAME>$**. For example, if your
> web server is called **WEBSERVERA** and belongs to the **UCCDMDOM** domain, the
> NETWORK SERVICE login would be **UCCDM\WEBSERVERA$**.

4. In the Object Explorer, expand the top-level **Security** folder. A list of folders is displayed.

5. Right-click the **Logins** folder and select **New Login**.

6. Ensure the **Windows authentication** option is selected and enter the NT
    AUTHORITY\NETWORK SERVICE account for the Side A web server in the form
    <DOMAIN>\<WEBSERVER MACHINE NAME>$.

7. In the **Select a page** pane on the left hand side, click **User Mapping**.

8. In the **Users mapped to this login** section, select the **Portal** database.

9. Ensure that the User column correctly contains the Network Service account for the web
    server.

10. In the **Database Role Membership** section, select the **portalapp** role, **portalrs** role and
    portalreporting role.

11. Click **OK**.

12. For deployments with multiple web servers, repeat step 5. to step 11. for each additional web
    server.

Upgrade and Configure Unified CCDM Components - Side A

Install the Database Components

On the Side A Database Server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information
    about the Unified CCDM Installer, see section "About the Unified CCDM Installer").

2. Select **Database Server**, and wait until the prerequisite checks have completed. If any
    checks fail, fix the issues as necessary.

3. When all checks have passed, click **Install**. At this point, the Informix client is installed first
    if necessary. If you see the Informix client installation screen, click **Install**.

4.   When the Informix client has been installed, the installation of the database components starts, and the **Setup** window displays.

5.   Click **Next** to go through each window in turn. You will need to enter the following details:

6.   In the **License Agreement** window:

   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.

7.   In the **Cryptography Configuration** window:

   - **Passphrase.** Enter the cryptographic passphrase you created during the installation of the Database Server component when you first installed Unified CCDM. If you continue installation with a new passphrase, you will be unable to access your existing data.

   - **Confirm Passphrase.** You will not be able to continue until the contents of this field are identical to the passphrase entered above.

   > **Warning!**
   >
   > You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you continue the installation with a new passphrase you will be unable to access your existing data.

8.   In the **Configure Database** window:

   - **Database Name**. Enter the name of the database catalog for Unified CCDM. By default this is **Portal**.

   - **Connect Using**. Select the login credentials you want to use:

      - **Windows Authentication Credentials of Application**. This is the recommended option.

      - **SQL Server Authentication using the login and password below**. This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your SQL Server Login Name and Password in the fields provided.

   - Click **Next**.

9.   In the **Destination Folder** window, if you want to change the location where the database components are stored, click **Change** and select the new location. The Unified CCDM components need to be installed in the same directory location on each of the servers.

10. Click **Install** to install the database components. During this process, the J2SE prerequisite will be automatically installed if it is not already present. If this happens, follow the screen

prompts to complete the J2SE installation. If you see a Security Alert dialog box during the installation, saying 'Revocation Information for the security certificate for this site is not available', click **Yes** to continue.

11. To install or upgrade your database immediately after installing the database components, select the **Launch Database Management Utility** check box at the end of the installation before clicking Finish.

12. Click **Finish**.

Upgrade the Portal Database

On the Side A Database Server:

1. If you selected the Launch Database Management Utility check box when you installed the database components, the Database Installer starts automatically after the installation. Otherwise, launch Unified CCDM **Database Installer**. The Database Installer is a wizard which guides you through the steps to upgrade the database.

2. Click **Next** to begin the upgrade process.

3. In the Database Setup Window choose **Upgrade an Existing Database**. Click **Next** to continue.

4. In the SQL Server Connection Details window, take the following actions:

    *   **Server Name**. Select the Microsoft SQL Server where the Unified CCDM database is located. In this case this is the machine running the application, and so it must be left as the default (local).

    *   **Database Name**. Enter or select the name of the database catalog that was originally used for the Unified CCDM database.

    *   **Connect Using**. Select the login credentials you want to use:

        *   The **Windows account information you use to log in to your computer**. This is the recommended option.

        *   The **Microsoft SQL Server login information assigned by the system administrator**. Only select this option if you are using a database catalog on a different domain. For this option you must enter your Login Name and Password in the fields provided.

    *   **Test Connection**. Click to make sure the connection to the Microsoft SQL Server is established. If you see the message 'Connection succeeded but database does not exist' then you must rectify this problem before continuing. Check that the database catalog name and security credentials are correct.

    *   When the database connection details have been tested and the connection is successful, click **Next**.

5. Click **Next** to perform the upgrade. The upgrade may take several minutes.

6.   When the Portal database upgrade is complete, click **Close** to close the Database Installer.

Install the App/Web Server

On the Side A App/Web Server:

1.   Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see section "About the Unified CCDM Installer").

2.   Select **App/Web Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.

3.   When all checks have passed, click **Install** to begin the App/Web Server installation. The **Domain Manager: Application Server Components** window displays.

4.   Click **Next** to go through each window in turn.

5.   If the **Domain Manager: Application Server Components** dialog is displayed, click **Install** to install the additional required components.

6.   If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.6 Framework is complete, restart the server to continue the installation of the App/Web Server.

7.   In the **License Agreement** window:

- **I accept the terms in the license agreement**. You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.

8.   In the **Cryptography Configuration** window:

- **Passphrase**. Enter the cryptographic passphrase you used for the installation of the Database Server component.

- **Confirm Passphrase**. You will not be able to continue until the contents of this field are identical to the passphrase entered above.

- Click **Next** to continue.

> **Warning!**
>
> You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you continue the installation with a new passphrase you will be unable to access your existing data.

9.   In the **Destination Folder** window, you can click **Change** to change the location where the App/Web Server components are installed. Click **Next** to continue.

10.   In the **Configure Database** window:

- **SQL Server Name**. Enter the host name or IP Address of the server hosting the Unified CCDM database. The default name of **localhost** is only valid if you are installing this component on the Database Server. Otherwise, specify the name of the Database Server. For a dual-sided deployment enter the name of the Side A Database server when installing the Side A components and enter the name of the Side B Database Server when installing the Side B components.

- **Catalog Name**. Enter or select the database catalog name you specified when installing the Database Server component. If you used the default value, this will be **Portal**.

- **Connect Using**. Select the login credentials you want to use:

  - **Windows authentication.** This is the recommended option.

  - **SQL Server authentication.** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter a SQL Server Login Name and Password in the fields provided.

- Click **Next** to continue.

11. Click **Install**.

12. When the installation has completed, click **Finish**. When installation is complete, the machine will restart.

Reconfigure the Unified CCDM Servers

Note

This step is only required if you have reinstalled Unified CCDM on new servers with different names. This step is not required if you have upgraded your existing servers, or have replaced your existing servers with new servers with the same names.

If the Unified CCDM server names have changed, the Unified CCDM cluster configuration must be updated to reference the new server names.

To update the cluster configuration, on the Side A Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCDM). In the **Database Connection** dialog box, set:

   - **Server Name**. Enter the name of the primary database server.

   - **Database Name**. Enter the name of the Unified 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.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

> **Note**
>
> If the Unified CCDM server names have changed, several errors may be reported when ICE starts for the first time after an upgrade. The steps in this section will fix the errors.

3. Select the **Setup** tab and click **Setup UCCDM Servers** to start the wizard. Click **Next** to go through each window in turn.

4. On the various **Configure Servers** pages, change the existing server name for each of the Unified CCDM servers to the new server name. The number of pages and servers to specify will depend on your deployment type. On each page, enter the following, then click **Next**:

    - **Primary Server**

        - **Server Name**. This is the non-domain qualified machine name.

        - **Server Address**. This defaults to Server Name. This can be changed to an IP Address or a domain qualified name of the server.

    - **Secondary Server**:

        - If you chose a dual-sided setup, provide the corresponding details for the Side B server.

5. Click **Next** and enter the relevant server information for each Unified CCDM server until you reach one of the following pages: **Primary Database Administrator Login**, **Secondary Database Administrator Login** or **Configure Relational Database Connection**.

6. Click **Next** to go through the remaining windows in turn, without changing anything.

7. When you see the confirmation message indicating that the wizard has completed successfully, click **Exit** to close the wizard.

8. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu.

9. In **ICE**, select the **Servers** tab. The list of servers will show both the old servers and the new servers. Right-click each of the old servers and select **Remove Server**.

10. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu. Exit ICE.

Reconfigure the Unified CCE Servers

> **Note**
>
> This step is only required if you have upgraded Unified CCE at the same time as upgrading Unified CCDM. This step is not required if you have not upgraded Unified CCE.

If you have upgraded Unified CCE at the same time upgrading Unified CCDM, the Unified CCDM cluster must be updated to ensure that Unified CCDM can communicate with Unified CCE. It may also be necessary to configure the Unified CCE Config Web Service, which wasn't present in some earlier versions of Unified CCE.

To reconfigure the Unified CCE servers after Unified CCE has been upgraded, on the Side A Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCDM). In the **Database Connection** dialog box, set:

    *   **Server Name**. Enter the name of the primary database server.

    *   **Database Name**. Enter the name of the Unified 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.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. Select the **Setup** tab and click **Configure Cisco Unified CCE Servers** to start the wizard.

4. On the **Select Task** page, select **Modify an existing instance**. Select the Unified CCE instance that has been updated, and click **Next** to go through each page in turn.

5. If you see the **Configure Primary Unified Config Web Service** page, enter or confirm the following details

    *   **URL**. This is the auto-generated URL of the primary Unified Config Web Service on the Unified CCE.

    *   **User Name**. This is a user name with appropriate access to the Unified CCE that the web service is running on. This user must be in the domain security group **<Server>_<UCCE-Instance>_Config**, where <Server> is the name of the server running Unified CCE and <UCCE-Instance> is the name of the Unified CCE Instance on this server.

    *   **Password**. This is the password for the user.

6. If you see the **Configure Primary ConAPI RMI Ports** page, enter or confirm the following ConAPI details:

    *   **Local Registry Port**. This is the port on the Unified CCE for the Unified 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.

7. If you see the **Configure ConAPI Application Instance** page enter the following details:

    - **Application Name.** The name of the application to be used for provisioning Unified CCE from Unified CCDM. Specify the name of the application you configured in section "Set Up ConAPI".

    - **Application Key.** Use the password for the application you specified above.

8. On the **Multi Media Support** page, if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance to provide support for non-voice interactions, select **Yes**. The default is No.

9. On the **Purge On Delete** page, if you want to purge items from Unified CCE automatically when they are deleted from Unified CCDM, select **Yes**. The default is Yes.

10. On the **Supervisor Active Directory Integration** page, if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors, select **Yes**. The default is No. If you select Yes, you will be prompted to provide Active Directory information so that Windows user accounts can be listed.

11. The Summary dialog box summarizes the details of the Unified CCE being configured and the settings you have chosen. Check the details, and if you are satisfied, click **Next**.

12. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.

13. For each remaining Unified CCE Server that has been upgraded, click **Configure Cisco Unified CCE Servers**, and repeat the steps above.

14. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu.

Reconfigure Unified CCE to Use the New Servers

> **Note**
>
> This step is only required if you have reinstalled Unified CCDM on new servers with different names. This step is not required if you have upgraded your existing servers, or have replaced your existing servers with new servers with the same names.

If you have reinstalled Unified CCDM on new servers with different names, Unified CCE must be updated to reference the new Unified CCDM servers.

To do this, on each Unified CCE instance in your Side A deployment:

1. Launch **CMS Control**. This opens the CMS control console.

2. On the **Application** tab, select the Unified CCDM database server and click **Edit**.

3. In the **Application connection details** tab, change the existing server name to the new server name. There are three places where this needs to be done:

- **Administration & Data Server Link**. The name of the newUnified CCDM Database Server, in capital letters, with **Server** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBServer**.

- **Application link**. The name of the new Unified CCDM Database Server, in capital letters, with **Client** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBClient**.

- **Application host name**. The name of the new Unified CCDM Database Server, in capital letters, for example, **PRODUCTDB**.

4. **Click** OK, then **OK** again to save the changes and exit CMS Control.

Post-Upgrade Actions

After you have upgraded Unified CCDM, complete the following post-installation steps:

- configure HTTPS as described in section "Configure SSL"

- bind server ports to IPv6 addresses as described in section section "Bind Server Ports to IPv6 Addresses"

- configure anti-virus operations as described in section "Configure Antivirus Options"

- implement the performance tuning steps described in section " Performance Tuning Checklists"

- complete the final post-installation actions described in section "Final Post-Installation Actions"

> **Note**
> If your installation uses single sign-on, the configuration is restored when the database is restored, so you do not need to reconfigure single sign-on as described in section "Configure Windows Login"

Restart and Validate (Side A)

Restart the Unified CCDM Services

Following an upgrade it is good practice to restart all Unified CCDM services.

Repeat the following steps on each upgraded Unified CCDM Database Server and each and upgraded Unified CCDM App/Web Server:

1. In the **Run** command dialog box, enter **Services.msc** and click **OK**.

2.   For each Unified CCDM service listed:

- if the selected service is in the Started state, right-click the service name and click **Restart**
- if the selected service is not started, right-click the service name and click **Start**.

Note

After starting the System Monitoring Service and Application Service on the App/Web Server, you will need to wait a few minutes before logging in to allow the services to load completely.

Validate the Upgrade

Check that the system is functional following the upgrade using the validation tests in section "Validating an Upgrade".

Checklist for Split Side Upgrades (Side B)

The second part of the split side upgrade applies the upgrade to Side B and restores replication.

Step	Complete
section "Prepare to Upgrade (Side B)"	
Stop the Unified CCDM services	
Backup the portal databases	
Configure new windows servers	
Apply optional security configuration	
section "Install SQL Server and Restore the Portal Database (Side B)"	
Install and configure SQL Server (Side B)	
Restore the portal database (Side B)	
Configure the SQL Agent user (Side B)	
Add network service accounts (Side B)	
section "Upgrade and Configure Unified CCDM Components - Side B"	
Install the Database Components	
Upgrade the portal database	
Install the App/Web Server	

Step	Complete
Reconfigure the Unified CCDM servers	
Reconfigure the Unified CCE Servers	
Reconfigure Unified CCE to use new servers	
section "Restore Replication"	
Stop forcing failover connections to the active side	
Configure Replication	
Monitor the replication snapshot	
Post-upgrade actions	
section "Restart and Validate (Side B)"	
Restart the Unified CCDM services	
Validate the upgrade	

Prepare to Upgrade (Side B)

Stop the Unified CCDM Services

Before starting the upgrade, you must stop all Unified CCDM services on all servers.

Stop the Unified CCDM Database Server Services

On the Side B Database Server:

1.   In **services.msc**, stop the **UCCDM: Data Import Server** service.

2.   Repeat this step for the UCCDM**: Partitioning Table Manager** service.

3.   Repeat this step for the UCCDM**: Provisioning Server** service.

Stop the Unified CCDM App/Web Server Services

On the Side B App/Web Server:

1.   In **services.msc**, stop the **UCCDM: System Monitoring Services** service.

2.   If you see a prompt saying that all other services will stop, and asking you if you want to continue, select **Yes**.

3.   If there are any other running Unified CCDM services, stop them too.

Back up the Portal Database

Back up the Portal database and copy the backup to a safe location where it can be accessed once the latest version of Unified CCDM has been installed on the new servers.

Identify the database to be backed up (see section "About a Split Sided Upgrade" for information about the options).

- If you are planning to restore the Side B database from the existing Side B database (option 1), you need to back up the existing Side B database now. So follow these instructions on the Side B Database Server.

- If you are planning to restore the Side B database from the upgraded Side A database (option 2), you need to back up the upgraded Side A database now. So follow these instructions on the Side A database server.

To back up the portal database, on the selected database server:

1. Launch **SQL Server Management Studio**.
2. Navigate to the Portal database.
3. Right-click **Portal** and select **Tasks > Backup**. Save the **.bak** file to a suitable location.
4. Close SQL Server Management Studio.

Configure New Windows Servers

On the new Side B servers running Windows Server 2012 R2, apply the Windows post-installation configuration in section "Windows Configuration".

Apply Optional Security Configuration

On the new Side B servers running Windows Server 2012 R2, apply the security settings described in section "Optional Security Configuration"

Uninstall Unified CCDM Components

Uninstall Unified CCDM Components as described in section "About Uninstalling Unified CCDM".

Install SQL Server and Restore the Portal Database (Side B)

Install and Configure SQL Server (Side B)

On the Side B Database Server:

1. Install SQL Server 2014 as described in section "Install SQL Server".

2. Configure the SQL Server network protocols as described in section "Configure SQL Server Network Protocols".

3. Configure the Windows Firewall for SQL Server as described in section "Configure Windows Firewall for SQL Server".

Restore the Portal Database (Side B)

Restore the Side B portal database from the database backup you made earlier (see section "Prepare to Upgrade (Side B)"). This backup may be a backup of the existing Side B database (option 1), or it may be a backup of the upgraded Side A database (option 2), depending on your requirements. See section "About a Split Sided Upgrade" for information about the backup and restore options for the Side B portal database.

On the Side B Database Server:

1. Launch **SQL Server Management Studio**.

2. Right-click the **Databases** folder and click **Restore Database**.

3. In the Restore Database window choose **From Device**, click **Add** and add the location of the database back up file you want to restore from. You may need to copy the backup file to a local file in order to access it. Click **OK**.

4. Select the check box next to the backup set you just added.

5. From the **To Database** drop-down list, select the **Portal** database as the restore destination.

6. Select **Options** and choose **Overwrite the existing database**. This will restore the database to the same location as the previous database. If you would like to choose a different location, update the **Restore As** path for each file to your preferred data file location.

7. Click **OK** to start the restore.

Configure the SQL Agent User (Side B)

For a dual-sided system, the SQL Agent User must be reconfigured.

On the Side B Database Server:

1. Launch **SQL Server Management Studio** and expand the **Security** folder. A list of subfolders is displayed.

2. Right-click the **Logins** folder and select **New Login**.

3. Ensure the **Windows authentication** option is selected and enter the SQL Agent User domain and login name in the form **<DOMAIN>\<LOGIN>**. This should be the user name that you specified for the SQL agent user account when you originally installed the portal database. For example, if your user is called **sql_agent_user** and belongs to the **CISCO** domain, enter **CISCO\sql_agent_user.**

4. In the **Select a page** pane on the left hand side, click **User Mapping**.

5. In the **Users mapped to this login** section, select the **Portal** database. The User column will auto-populate with the domain user name for the SQL Agent User.

6. In the **Database Role Membership** section, select the **db_owner** role.

7. Click **OK** to apply the changes.

Add Network Service Accounts (Side B)

You must add the NETWORK SERVICE account for all web servers to the database logins with appropriate access permissions. Before this can be done the existing accounts must be deleted from the Portal database logins.

On the Side B Database Server:

1. Launch **SQL Server Management Studio** and in the Object Explorer, expand the **Portal** database. A list of folders is displayed.

2. Expand the **Portal > Security > Users** folder. A list of database logins is displayed.

3. For each occurrence of the **NETWORK SERVICE** account for a remote web server in the deployment, right-click it and select **Delete**.

> **Note**
>
> Do not delete the entry for the NETWORK SERVICE account for the local machine (**NT AUTHORITY\NETWORK SERVICE**).
>
> The NETWORK SERVICE logins for remote web server machines in the deployment are of the form **<DOMAIN>\<WEBSERVER MACHINE NAME>$**. For example, if your web server is called **WEBSERVERA** and belongs to the **UCCDMDOM** domain, the NETWORK SERVICE login would be **UCCDM\WEBSERVERA$**.

4. In the Object Explorer, expand the top-level **Security** folder. A list of folders is displayed.

5. Right-click the **Logins** folder and select **New Login**.

6. Ensure the **Windows authentication** option is selected and enter the NT AUTHORITY\NETWORK SERVICE account for the Side A web server in the form **<DOMAIN>\<WEBSERVER MACHINE NAME>$.**

7. In the **Select a page** pane on the left hand side, click **User Mapping**.

8. In the **Users mapped to this login** section, select the **Portal** database.

9. Ensure that the User column correctly contains the Network Service account for the web server.

10. In the **Database Role Membership** section, select the **portalapp** role, **portalrs** role and **portalreporting** role.

11. Click **OK**.

12.   For deployments with multiple web servers, repeat step 5. to step 11. for each additional web
      server.

Configure Replication Share

For a dual-sided system, the replication share folder must be reconfigured.

On the Side B Database Server:

1.   In the SQL Server installation folder, locate the replication folder. Typically this is located
      at **C:\Program Files\Microsoft SQL
      Server\MSSQL12.MSSQLSERVER\MSSQL\repldata**.

2.   Create a share for this folder, giving the **Everyone** group full control to the share, as
      follows:

      a.   Right-click on the replication folder and select **Share With > Advanced sharing**.

      b.   On the **Sharing** tab, click **Advanced Sharing**.

      c.   Select **Share this folder** and specify the share name as the name that was used for the
            replication folder when you originally installed the portal database. The default name is
            ReplData.

      d.   Click **Permissions**, select the group **Everyone**, and allow all permissions.

3.   Click **OK** to apply the changes.

Upgrade and Configure Unified CCDM Components - Side B

Install the Database Components

On the Side B Database Server:

1.   Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information
      about the Unified CCDM Installer, see section "About the Unified CCDM Installer").

2.   Select **Database Server**, and wait until the prerequisite checks have completed. If any
      checks fail, fix the issues as necessary.

3.   When all checks have passed, click **Install**. At this point, the Informix client is installed first
      if necessary. If you see the Informix client installation screen, click **Install**.

4.   When the Informix client has been installed, the installation of the database components
      starts, and the **Setup** window displays.

5.   Click **Next** to go through each window in turn. You will need to enter the following details:

6.   In the **License Agreement** window:

- **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.

7. In the **Cryptography Configuration** window:

   - **Passphrase.** Enter the cryptographic passphrase you created during the installation of the Database Server component when you first installed Unified CCDM. If you continue installation with a new passphrase, you will be unable to access your existing data.

   - **Confirm Passphrase.** You will not be able to continue until the contents of this field are identical to the passphrase entered above.

   > **Warning!**
   >
   > You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you continue the installation with a new passphrase you will be unable to access your existing data.

8. In the **Configure Database** window:

   - **Database Name**. Enter the name of the database catalog for Unified CCDM. By default this is **Portal**.

   - **Connect Using**. Select the login credentials you want to use:

     - **Windows Authentication Credentials of Application**. This is the recommended option.

     - **SQL Server Authentication using the login and password below**. This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your SQL Server Login Name and Password in the fields provided.

   - Click **Next**.

9. In the **Destination Folder** window, if you want to change the location where the database components are stored, click **Change** and select the new location. The Unified CCDM components need to be installed in the same directory location on each of the servers.

10. Click **Install** to install the database components. During this process, the J2SE prerequisite will be automatically installed if it is not already present. If this happens, follow the screen prompts to complete the J2SE installation. If you see a Security Alert dialog box during the installation, saying 'Revocation Information for the security certificate for this site is not available', click **Yes** to continue.

11. To install or upgrade your database immediately after installing the database components, select the **Launch Database Management Utility** check box at the end of the installation before clicking Finish.

12.   Click **Finish**.

Upgrade the Portal Database

> **Note**
>
> This step only required if you opted to restore the Side B portal database from a backup of the old Side B database (option 1). It is not required if you restored the Side B portal database from a backup of the existing Side A database (option 2). See section "About a Split Sided Upgrade" for information about the backup and restore options for the Side B portal database.

On the Side B Database Server:

1.   If you selected the Launch Database Management Utility check box when you installed the database components, the Database Installer starts automatically after the installation. Otherwise, launch Unified CCDM **Database Installer**. The Database Installer is a wizard which guides you through the steps to upgrade the database.

2.   Click **Next** to begin the upgrade process.

3.   In the Database Setup Window choose **Upgrade an Existing Database**. Click **Next** to continue.

4.   In the SQL Server Connection Details window, take the following actions:

   - **Server Name**. Select the Microsoft SQL Server where the Unified CCDM database is located. In this case this is the machine running the application, and so it must be left as the default (local).

   - **Database Name**. Enter or select the name of the database catalog that was originally used for the Unified CCDM database.

   - **Connect Using**. Select the login credentials you want to use:

      - The **Windows account information you use to log in to your computer**. This is the recommended option.

      - The **Microsoft SQL Server login information assigned by the system administrator**. Only select this option if you are using a database catalog on a different domain. For this option you must enter your Login Name and Password in the fields provided.

   - **Test Connection**. Click to make sure the connection to the Microsoft SQL Server is established. If you see the message 'Connection succeeded but database does not exist' then you must rectify this problem before continuing. Check that the database catalog name and security credentials are correct.

   - When the database connection details have been tested and the connection is successful, click **Next**.

5.   Click **Next** to perform the upgrade. The upgrade may take several minutes.

6. When the Portal database upgrade is complete, click **Close** to close the Database Installer.

Install the App/Web Server

On the Side B App/Web Server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see section "About the Unified CCDM Installer").

2. Select **App/Web Server**, and wait until the prerequisite checks have completed. If any checks fail, fix the issues as necessary.

3. When all checks have passed, click **Install** to begin the App/Web Server installation. The **Domain Manager: Application Server Components** window displays.

4. Click **Next** to go through each window in turn.

5. If the **Domain Manager: Application Server Components** dialog is displayed, click **Install** to install the additional required components.

6. If the Microsoft .NET 4.5 Framework prerequisite is missing, it will be installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.6 Framework is complete, restart the server to continue the installation of the App/Web Server.

7. In the **License Agreement** window:

    •   **I accept the terms in the license agreement**. You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting.

8. In the **Cryptography Configuration** window:

    •   **Passphrase**. Enter the cryptographic passphrase you used for the installation of the Database Server component.

    •   **Confirm Passphrase**. You will not be able to continue until the contents of this field are identical to the passphrase entered above.

    •   Click **Next** to continue.

    > **Warning!**
    > You must use the same cryptographic passphrase as was originally used when Unified CCDM was first installed. If you continue the installation with a new passphrase you will be unable to access your existing data.

9. In the **Destination Folder** window, you can click **Change** to change the location where the App/Web Server components are installed. Click **Next** to continue.

10. In the **Configure Database** window:

- **SQL Server Name**. Enter the host name or IP Address of the server hosting the Unified CCDM database. The default name of **localhost** is only valid if you are installing this component on the Database Server. Otherwise, specify the name of the Database Server. For a dual-sided deployment enter the name of the Side A Database server when installing the Side A components and enter the name of the Side B Database Server when installing the Side B components.

- **Catalog Name**. Enter or select the database catalog name you specified when installing the Database Server component. If you used the default value, this will be **Portal**.

- **Connect Using**. Select the login credentials you want to use:

    - **Windows authentication.** This is the recommended option.

    - **SQL Server authentication.** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter a SQL Server Login Name and Password in the fields provided.

- Click **Next** to continue.

11. Click **Install**.

12. When the installation has completed, click **Finish**. When installation is complete, the machine will restart.

Reconfigure the Unified CCDM Servers

Note

This step is only required if you have reinstalled Unified CCDM on new servers with different names. This step is not required if you have upgraded your existing servers, or have replaced your existing servers with new servers with the same names.

If the Unified CCDM server names have changed, the Unified CCDM cluster configuration must be updated to reference the new server names.

These steps are required the Side B database server, although these values will be overwritten later from the values on Side A when replication is reinstated. To update the cluster configuration, on the Side B Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCDM). In the **Database Connection** dialog box, set:

- **Server Name**. Enter the name of the primary database server.

- **Database Name**. Enter the name of the Unified 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.

2.   Click **OK**. The ICE Cluster Configuration tool starts by default.

> **Note**
>
> If the Unified CCDM server names have changed, several errors may be reported when ICE starts for the first time after an upgrade. The steps in this section will fix the errors.

3.   Select the **Setup** tab and click **Setup UCCDM Servers** to start the wizard. Click **Next** to go through each window in turn.

4.   On the various **Configure Servers** pages, change the existing server name for each of the Unified CCDM servers to the new server name. The number of pages and servers to specify will depend on your deployment type. On each page, enter the following, then click **Next**:

   - **Primary Server**
       - **Server Name**. This is the non-domain qualified machine name.
       - **Server Address**. This defaults to Server Name. This can be changed to an IP Address or a domain qualified name of the server.
   - **Secondary Server**:
       - If you chose a dual-sided setup, provide the corresponding details for the Side B server.

5.   Click **Next** and enter the relevant server information for each Unified CCDM server until you reach one of the following pages: **Primary Database Administrator Login**, **Secondary Database Administrator Login** or **Configure Relational Database Connection**.

6.   Click **Next** to go through the remaining windows in turn, without changing anything.

7.   When you see the confirmation message indicating that the wizard has completed successfully, click **Exit** to close the wizard.

8.   To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu.

9.   In **ICE**, select the **Servers** tab. The list of servers will show both the old servers and the new servers. Right-click each of the old servers and select **Remove Server**.

10. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu. Exit ICE.

Reconfigure the Unified CCE Servers

> **Note**
>
> This step is only required if you have upgraded Unified CCE at the same time as upgrading Unified CCDM. This step is not required if you have not upgraded Unified CCE.

If you have upgraded Unified CCE at the same time upgrading Unified CCDM, the Unified CCDM cluster must be updated to ensure that Unified CCDM can communicate with Unified CCE. It may also be necessary to configure the Unified CCE Config Web Service, which wasn't present in some earlier versions of Unified CCE.

These steps are required the Side B database server, although these values will be overwritten later from the values on Side A when replication is reinstated. To reconfigure the Unified CCE servers after Unified CCE has been upgraded, on the Side B Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCDM). In the **Database Connection** dialog box, set:

    *   **Server Name**. Enter the name of the primary database server.

    *   **Database Name**. Enter the name of the Unified 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.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. Select the **Setup** tab and click **Configure Cisco Unified CCE Servers** to start the wizard.

4. On the **Select Task** page, select **Modify an existing instance**. Select the Unified CCE instance that has been updated, and click **Next** to go through each page in turn.

5. If you see the **Configure Primary Unified Config Web Service** page, enter or confirm the following details

    *   **URL**. This is the auto-generated URL of the primary Unified Config Web Service on the Unified CCE.

    *   **User Name**. This is a user name with appropriate access to the Unified CCE that the web service is running on. This user must be in the domain security group **<Server>_<UCCE-Instance>_Config**, where <Server> is the name of the server running Unified CCE and <UCCE-Instance> is the name of the Unified CCE Instance on this server.

    *   **Password**. This is the password for the user.

6. If you see the **Configure Primary ConAPI RMI Ports** page, enter or confirm the following ConAPI details:

    *   **Local Registry Port**. This is the port on the Unified CCE for the Unified 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.

7. If you see the **Configure ConAPI Application Instance** page enter the following details:

    • **Application Name.** The name of the application to be used for provisioning Unified
      CCE from Unified CCDM. Specify the name of the application you configured in
      section "Set Up ConAPI".

    • **Application Key.** Use the password for the application you specified above.

8. On the **Multi Media Support** page, if you are using a Cisco Unified Web and E-Mail
    Interaction Manager application instance to provide support for non-voice interactions, select
    Yes. The default is No.

9. On the **Purge On Delete** page, if you want to purge items from Unified CCE automatically
    when they are deleted from Unified CCDM, select **Yes**. The default is Yes.

10. On the **Supervisor Active Directory Integration** page, if you want to enable support for
    associating existing Active Directory user accounts for Unified CCE Supervisors, select
    Yes. The default is No. If you select Yes, you will be prompted to provide Active Directory
    information so that Windows user accounts can be listed.

11. The Summary dialog box summarizes the details of the Unified CCE being configured and
    the settings you have chosen. Check the details, and if you are satisfied, click **Next**.

12. A confirmation message is displayed to indicate that the wizard has completed successfully.
    Click **Exit** to close the wizard.

13. For each remaining Unified CCE Server that has been upgraded, click **Configure Cisco
    Unified CCE Servers**, and repeat the steps above.

14. To save and action your changes, either click the **Save** icon in the tool bar or select **File >
    Save** from the menu.

Reconfigure Unified CCE to Use the New Servers

> **Note**
> This step is only required if you have reinstalled Unified CCDM on new servers with different
> names. This step is not required if you have upgraded your existing servers, or have replaced
> your existing servers with new servers with the same names.

If you have reinstalled Unified CCDM on new servers with different names, Unified CCE must
be updated to reference the new Unified CCDM servers.

To do this, on each Unified CCE instance in your Side B deployment:

1. Launch **CMS Control**. This opens the CMS control console.

2. On the **Application** tab, select the Unified CCDM database server and click **Edit**.

3. In the **Application connection details** tab, change the existing server name to the new
    server name. There are three places where this needs to be done:

- **Administration & Data Server Link**. The name of the newUnified CCDM Database Server, in capital letters, with **Server** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBServer**.

- **Application link**. The name of the new Unified CCDM Database Server, in capital letters, with **Client** appended. For example, if your Database Server is **PRODUCTDB**, enter **PRODUCTDBClient**.

- **Application host name**. The name of the new Unified CCDM Database Server, in capital letters, for example, **PRODUCTDB**.

4. **Click** OK, then **OK** again to save the changes and exit CMS Control.

Restore Replication

Stop Forcing Failover Connections to the Active Side

To stop forcing the failover connections to the active side:

1. Remove the entries to the **hosts** files you made in section "Prepare to Upgrade (Side A)".

Configure Replication

Replication between the databases is set up and monitored using the Replication Manager application which is available in the Unified CCDM Integrated Configuration Environment (ICE) tool.

> **Note**
>
> The user running Replication Manager must have administrator permissions in both Windows and SQL Server, for both the publisher and the subscriber Database Servers.
>
> Usually, the publisher will be the Side A Database Server, but occasionally, it may be necessary to configure the Side B Database Server as the publisher.

To configure replication, on the publisher Database Server:

1. Launch **Integrated Configuration Environment** (installed as part of Unified CCDM). In the **Database Connection** dialog box, set:

   - **Server Name**. Enter the name of the primary database server.

   - **Database Name**. Enter the name of the Unified 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.

2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. From the Tool drop-down list, select **Replication Manager**. The Replication Manager opens in the Setup tab. The Setup tab has the following sections:

    - **Unified CCDM Database Server Properties** contains the publisher and subscriber Unified CCDM database details.

    - **Distributor Properties** contains the SQL Server Replication distributor properties.

    The default values shown in the Setup tab are derived from the values initially configured in the Cluster Configuration tool and will be suitable in most cases.

4. If required, modify the Unified CCDM Database Server Properties.

    - **Server Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.

    - **Catalog Name** (publisher and subscriber). This is the value specified in ICE Cluster Configuration. It may be changed, but if so, a valid database with the new name must already exist on the corresponding server.

5. The Identity Server should be replicated by default. To replicate the Identity Server Database, click the **Identity Database Replication Enabled** checkbox.

6. If required, modify the distributor properties.

    - **Server Name**. The name of the subscriber server hosting the Unified CCDM database. This is the value specified in ICE Cluster Configuration and cannot be changed in Replication Manager.

    - **Catalog Name**. The name to be assigned to the distribution database. The recommended value is **distribution_portal**.

    - **Data Folder**. The folder path on the distributor server where the data file for the distribution database will be created.

    > **Note**
    >
    > If you are setting up replication after performing an upgrade, be particularly careful with the Data Folder path, as it may be different from the value used in previous versions of Unified CCDM. Make sure you use the path that was specified when the database was set up.

    - **Log Folder**. The folder path on the distributor server where the transaction log file for the distribution database will be created.

    - **Distribution Share**. The distribution share folder where replication snapshot files will be generated.

    - **Override Distributor Admin Password**. Select to override the auto-generated replication password which will be used to establish connectivity. The auto-generated password is 14 characters long, and will contain alpha-numeric characters (both upper

and lower case) and a special character. If this does not meet the complexity requirements of the server then select this option and specify a password of your choice.

7. When you have set the required replication properties, click **Configure** to configure replication.

8. You may be prompted to save pending changes to the database before continuing. If so, click **Yes** to save pending changes and continue.

9. It may take several minutes to configure replication. Once replication has been configured, the Replication Manager automatically switches to the Monitor tab, which enables you to monitor the progress of the replication snapshot.

Monitor the Replication Snapshot

> **Note**
>
> The subscriber Database Server is not available for use until the replication snapshot has completed and all the data has been copied from the publisher to the subscriber.
>
> The time taken for the replication snapshot to complete depends on the volume of data in the publisher database and the bandwidth between the servers. For a large database, this may take several hours.

To monitor the progress of the replication snapshot:

1. In the ICE Replication Manager, select the **Monitor** tab. The Monitor tab has the following panes:

    *   **Publications** (top left) lists the publisher servers and the publications on each publisher that need to be shared with the subscribers.

    *   **Subscriptions and Agents** (top right) shows the subscriptions to a publication and the replication agents associated with a publication. This pane has two tabs, Subscriptions and Agents.

    *   **Subscriptions** shows the subscriptions to the selected publication. You can right-click on a subscription to start or stop the subscription.

    *   **Agents** shows the replication agents associated with the selected publication. You can right-click on a replication agent to start or stop the agent.

    *   **Sessions** (bottom left) shows all sessions for the selected publication and replication agent in the last 24 hours.

    *   **Actions** (bottom right) shows the activity for the selected session.

2. In the top left hand pane, select the first Unified CCDM database publication from the list of publications. If you have used the default database name, this will start with **[Portal]**.

3. Wait for the replication snapshot for this publication to complete.

To check the replication status for a Unified CCDM database publication, in the bottom right hand pane of the Monitor tab, inspect the messages in the Action Message list. Once the replication snapshot is complete and replication is operational for a publication, you will see the following two messages:

"Delivered snapshot from . . . "

"No replicated transactions are available".

After this, the second message is replaced with messages showing new replicated transactions as they are sent through the system, for example:

"4 transaction(s) with 14 command(s) were delivered".

4.   Repeat the two steps above for each of the remaining Unified CCDM database publications.

5.   When replication is complete for all portal database publications, close the ICE tool.

The subscriber database can now be used to service requests. For more information about the Replication Manager see the *Integrated Configuration Environment (ICE) for Cisco Unified Contact Center Domain Manager*.

Post-Upgrade Actions

After you have upgraded Unified CCDM, complete the following post-installation steps:

- configure HTTPS as described in section "Configure SSL"
- bind server ports to IPv6 addresses as described in section section "Bind Server Ports to IPv6 Addresses"
- configure anti-virus operations as described in section "Configure Antivirus Options"
- implement the performance tuning steps described in section " Performance Tuning Checklists"
- complete the final post-installation actions described in section "Final Post-Installation Actions"

Note

If your installation uses single sign-on, the configuration is restored when the database is restored, so you do not need to reconfigure single sign-on as described in section "Configure Windows Login"

Restart and Validate (Side B)

Restart the Unified CCDM Services

Following an upgrade it is good practice to restart all Unified CCDM services.

Repeat the following steps on each upgraded Unified CCDM Database Server and each and upgraded Unified CCDM App/Web Server:

1.   In the **Run** command dialog box, enter **Services.msc** and click **OK**.

2.   For each Unified CCDM service listed:

- if the selected service is in the Started state, right-click the service name and click **Restart**

- if the selected service is not started, right-click the service name and click **Start**.

> **Note**
>
> After starting the System Monitoring Service and Application Service on the App/Web Server, you will need to wait a few minutes before logging in to allow the services to load completely.

Validate the Upgrade

Check that the system is functional following the upgrade using the validation tests in section "Validating an Upgrade".

Uninstalling Unified CCDM

About Uninstalling Unified CCDM

This chapter describes how to remove the Unified CCDM components from the platform.

To uninstall Unified CCDM, firstly you must remove the database components. This removes the ability to import and provision data between remote data sources (such as Unified CCE or Unified Communications Manager) and the Unified CCDM Database.

Uninstallation involves the following steps:

- removing database replication (dual-sided systems only)
- uninstalling the database components
- removing the database catalog (only if Unified CCDM is being removed permanently)
- uninstalling the other Unified CCDM components.

Remove Database Replication

Note

This step is only required if you have a dual-sided system.

If you have a dual-sided installation then you must remove database replication before removing the database components.

Before removing database replication:

1. Ensure that the database is in a consistent state.
2. Stop all Unified CCDM Services on all servers.

To remove database replication:

1. Ensure you are logged in to the Side A Database Server as a domain level user with administrative rights over both Database Servers.

2. Launch **Integrated Configuration Environment** (installed as part of Unified CCDM). In the **Database Connection** dialog box, set:

   - **Server Name**. Enter the name of the primary database server.
   - **Database Name**. Enter the name of the Unified 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**. The ICE Cluster Configuration tool starts by default.

4. From the Tool drop-down list select **Replication Manager**.

5. Click the **Setup** tab to see the replication setup details.

6. Click **Disable** to remove replication from the Unified CCDM database. When prompted, click **Yes** to proceed with replication removal.

7. Replication removal may take several minutes. Wait for the 'Replication Removed' message to display in the Output Window and then exit ICE.

Uninstall Application Components

To uninstall the applicationUnified CCDM components:

1. On the Side A App/Web Server, launch **Control Panel** and select **Programs and Features**.

2. Select **Domain Manager: Application Server Components.**

3. Click **Uninstall.**

4. For a dual-sided deployment, repeat step 1. to step 3. on the Side B App/Web Server.

> **Note**
> After the uninstallation is complete, delete the installation folder that contains the log files and folders from the following location: C:\Program Files\Domain Manager. Before deleting this folder, make sure there are no other components installed on the system.

Uninstall the Database Components

To uninstall the database components, on the Database Server:

1. Launch **Control Panel** and select **Uninstall a program.**

2. Select **Domain Manager: Database Components.**

3. Click **Uninstall.**

4. For a dual-sided deployment, repeat these steps on the Side B Database Server.

> **Note**
> After the uninstallation is complete, delete the installation folder that contains the log files and folders from the following location: C:\Program Files\Domain Manager. Before deleting this folder, make sure there are no other components installed on the system.

Uninstalling the database components does not remove the Unified CCDM database catalog.

Remove the Database Catalog

Warning!

Do not remove the database catalog from your system unless you intend to permanently remove Unified CCDM, or you have been instructed to do so by your vendor support.

To remove the Unified CCDM database catalog, you will need to use SQL Server Management Studio, as follows:

1. Launch **SQL Server 2014 Management Studio** and connect to the local Database Server.

2. 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**.

3. The Delete Database window displays.

4. Select the **Close existing connections** check box.

5. Click **OK**.

This permanently removes the database catalog.

Troubleshooting

About Installer Logs

Unified CCDM installers are launched with logging enabled. Install logs are located in **C:\InstallLogs** for both the Database and App/Web Server installers.

Changing the SQL Server Installation Language to US English

If the step to install the portal database fails with an error

Exception in installation: [SQL Server language must be US English]

you must change the SQL Server language to US English before the installation can continue. To do this, on the database server, run the following T-SQL scripts in the order below.

Script 1

```
USE master;
GO
DECLARE @LANGUAGE AS NVARCHAR(MAX);
SELECT @LANGUAGE = 'EXEC sp_configure '+CHAR(39)+'default language'+CHAR(39)+',
'+CAST([langid] AS VARCHAR(2))+';'
FROM sys.syslanguages
WHERE name = 'us_english';
EXECUTE sp_executesql @LANGUAGE;
GO
```

Script 2

```
RECONFIGURE WITH OVERRIDE;
GO
```

Script 3

```
USE [master];
ALTER LOGIN [<username>] WITH DEFAULT_LANGUAGE=[us_english];
GO
```

where *<username>* is the Windows domain user or SQL Server user you will specify for the **Connect Using** option during the installation of the Portal Database (**SQL Server Connection Details** window). For example:

- if you will connect using the option **The Windows account information I use to logon to my computer**, and have a user name **user1** on **Unified CCDMDOM**, you would enter **Unified CCDMDOM\user1** for *<username>*

- if you will connect using the option **The SQL Server login information assigned by the system administrator**, and will use the **sa** user, you would enter **sa** for *<username>*.