Installation and Configuration Guide for Cisco Unified Contact Center Domain Manager, Release 12.5(1)

For Unified Contact Center Enterprise

First Published: January, 2020
Last Updated: December, 2022

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Installation and Configuration Guide for Cisco Unified Contact Center Domain Manager: For Unified Contact Center Enterprise. December 30, 2022

Contents

Preface

About This Guide

Installation and Configuration Guide for Cisco Unified Contact Center Domain Manager explains the installation and configuration process of Unified Contact Center Domain Manager (Unified CCDM). Read this document carefully before proceeding and ensure that it is available to anyone installing, configuring or managing Unified Contact Center Domain Manager.

Who Should Read This Document

This document should be read by anyone who needs to install, configure or manage Unified CCDM. It is intended for network administrators who are familiar with contact center operations and management, network services and routing operations and administration. An understanding of SQL Server database administration is also helpful.

Change History

This table lists changes made to this guide. Most recent changes appear at the top.

Change	See	Date
Added a note under **Security Considerations**	"Security Considerations" on page 25	December, 2022
Added a new section: **Configure Replication Share Folder**	"Configure Replication Share Folder" on page 68	October, 2022
Updated important note in the **Configuring Windows Authentication** section.	"Configuring Windows Authentication" on page 62	
Removed Allow Specific File Extensions in IIS section	-	August, 2021
Removed section on Diagnostic Framework	-	May, 2021
Edge added to supported list of browsers	"User Desktop Requirements" on page 20	February, 2021
Troubleshooting steps added for portal login errors	"Portal Login Error Messages" on page 130	
Important note about Diagnostic Framework being optional added	-	May, 2019

Product Naming Conventions

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

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

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

Related Documentation

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

Related documentation includes the documentation sets for:

- Cisco CTI Object Server (CTIOS), Cisco Agent Desktop (CAD)
- Cisco Agent Desktop - Browser Edition (CAD-BE)
- Cisco Unified Contact Center Management Portal
- Cisco Unified Customer Voice Portal (CVP)
- Cisco Unified IP IVR, Cisco Unified Intelligence Center
- Cisco Support Tools

Documentation for these Cisco Unified Contact Center products is accessible from:

- https://www.cisco.com/cisco/web/psa/default.html.

Documentation for Cisco Unified Communications Manager is accessible from:

- https://www.cisco.com/cisco/web/psa/default.html.

Technical Support documentation and tools are accessible from:

- https://www.cisco.com/en/US/support/index.html.

The Product Alert tool is accessible from (sign in required):

- https://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice.

For information on the Cisco software support methodology, refer to *Software Release and Support Methodology: ICM/IPCC,* available from (sign in required):

- https://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/prod_bulletins_list.html.

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

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

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

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 https://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.

Document Conventions

This guide uses the following typographical conventions.

Convention	Indicates
Italic	Emphasis, or the title of a published document.
Bold	An item in the user interface, such as a window, button, or tab.
`Monospace`	A file name or command.
Script	A variable, which is a placeholder for user-specific text provided by the user. Or, text that must be typed by the user.

Document conventions

1 Planning Your Installation

About the 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**.
- Dedicated **Admin Workstation CMS Server.**

Infrastructure Software

Unified CCDM requires:

- **Windows Server 2016**
- **SQL Server 2016 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). It consists of:
  - The **Portal Database**, which holds the data that has been provisioned through Unified CCDM or imported from Unified CCE.
  - The **Identity (IdSvr3Config) Database** holds the data security token which is used to authenticate users via single sign-on.
  - 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:
  - The **Application Server** delivers application services such as search, security and resilience to the Unified CCDM Web Server.
  - The **Web Server** provides the web front end that enables users to perform resource management and administrative tasks.
- The **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 Model

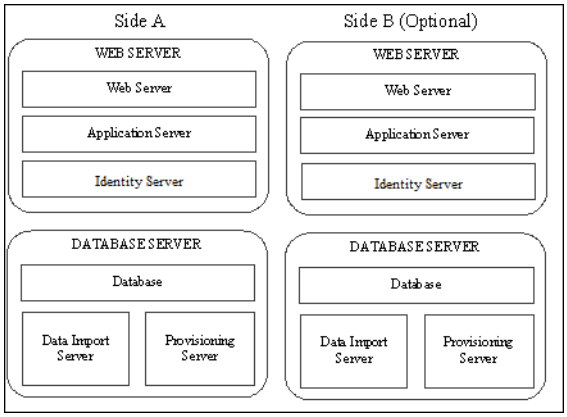
In many environments, Unified CCDM is installed using a dual-sided deployment model to provide load balancing, resiliency, and high availability. For deployments that require layered security, such as Internet-facing environments, both sides are split across separate Database Servers and App/Web Servers 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. Refer to the Virtualization Wiki for Hardware and System Software Specification:
https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/ccdmvirt.html

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

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

The following image 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.



Component layout for a dual-sided two-tier deployment

2 Installation Requirements

About the Installation Prerequisites

This chapter describes the installation prerequisites 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 and can be up to a maximum of 15 characters. The name must conform to the **NETBIOS guidelines** (https://support.microsoft.com/en-in/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and).
- 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.
- The SQL Server **TempDB** directory and **TempDB** log directory should not be located on the same disk as the operating system.

Windows Requirements

- All Unified CCDM servers require the **Windows Server 2016** version of Windows.

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://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server?view=sql-server-2017

Database Servers

The Unified CCDM Database Server requires **Microsoft SQL Server 2016 64-bit, Service Pack 2, Standard Edition**. The following components should be deployed:

- **Database Engine**
- **SQL Server Management Studio**

Application Servers

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

Java Runtime Environment Support

Cisco Unified CCE Resource Management functionality requires Java Runtime Environment support. Unified CCDM supports:

- Open JDK11. If a version prior to this update is installed, the application automatically installs this JDK update.

Minor version JDK updates can be applied. Major version updates are not supported.

User Desktop Requirements

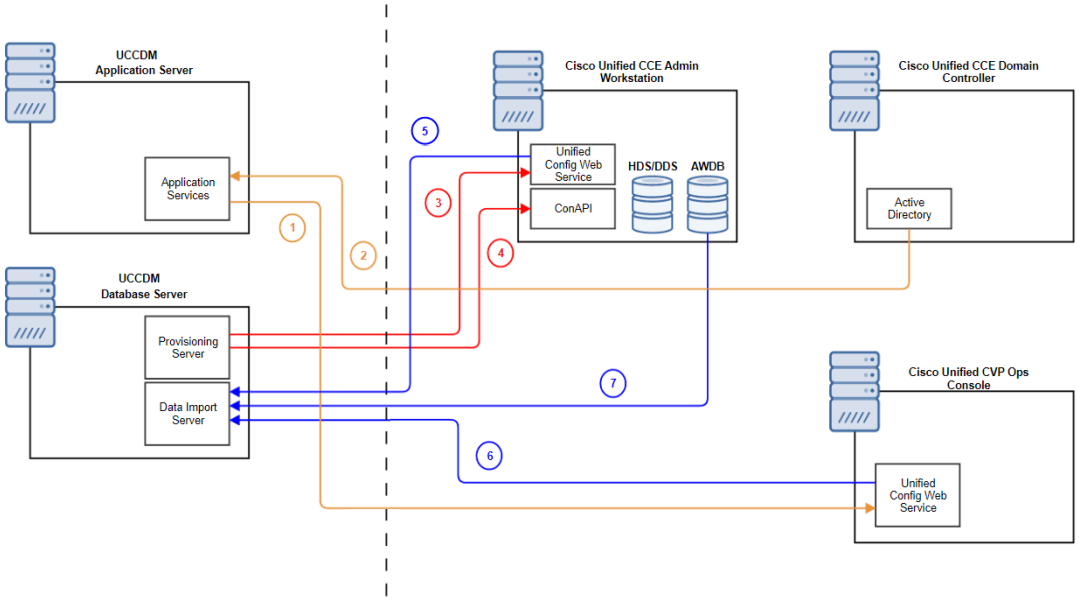
The Unified CCDM web application supports the following browsers:

- Google Chrome (Version 76.0.3809.100 (Official Build) (64-bit))
- Internet Explorer version 11
- Microsoft Edge version 88
- Mozilla Firefox version 68.0.2 (64-bit)

Important: **The Unified CCDM web application may not work with virtual desktops or application virtualization 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.**

Architecture Diagram

This section provides details of the standard connections from Unified CCDM components to all remote telephony equipment from Cisco.



Purpose	Local Server	Local Component	Remote Server	Remote Component	Protocol	Default Local Port	Default Remote Ports
Media File Upload/Download VXML Application Upload	CCDM Application Server	Application Services	Cisco Unified CVP Ops Console	Unified Config	HTTPS (REST Web Service)		8111*
Supervisor domain account provisioning	CCDM Application Server	Application Services	Cisco CCE Domain Controller	Active Directory	TCP (LDAP)		389
Provisioning Precision Queues, Agent Attributes, and so on	CCDM Database Server	Provisioning Service	Cisco Unified CCE Admin Workstation	Unified Config	HTTPS (REST Web Service)		443

Purpose	Local Server	Local Component	Remote Server	Remote Component	Protocol	Default Local Port	Default Remote Ports
Provisioning Agents, Skillgroups, and so on	CCDM Database Server	Provisioning Service	Cisco Unified CCE Admin Workstation	ConAPI	TCP (Java Remoting)	Local Registry - 2099* Local Port - 3333*	Remote Registry - 2099*
Importing Capacity Data	CCDM Database Server	Data Import Service	Cisco Unified CCE Admin Workstation	Unified Config	HTTPS (REST Web Service)		443
Importing Media Files, Media Servers, and so on	CCDM Database Server	Data Import Service	Cisco Unified CVP Ops Console	Unified Config	HTTPS (REST Web Service)		8111*
Importing Agents, Skillgroups, and so on	CCDM Database Server	Data Import Service	Cisco Unified CCE Admin Workstation	AWDB	TCP (MS SQL Server)		1433

** Ports configurable via Integrated Configuration Environment (ICE) tool on CCDM Database Server*

Firewall Configurations

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. Port restrictions should be limited to only the servers that require the specified communication 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

* These are the default ports. If you are using different ports, then the default ports can be disabled.

Unified CCDM Database Server Port Usage

Application Protocol/Service	Protocol	Incoming Ports	Used by	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	TCP	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
ConAPI Local Registry	TCP	2099**	Unified CCE Admin Workstation	Provisioning
ConAPI Local Registry	TCP	2098+	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.

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

*** This is the default port. If you are using different port, then the default port can be disabled.

+ 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, Application Servers	Importing Dimension and Fact Data, Provisioning Activities
ConAPI Remote Registry	TCP	2099*	Database Servers	Provisioning
ConAPI Remote Registry	TCP	2098+	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.

+ Default value for Side B – use configured in Cluster Configuration.

** These are the default ports. If you are using different ports, then the default ports can be disabled.

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 Communications Manager Port Usage

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

* This is the default port. If you are using a different port, then the default port can be disabled.

Cisco Unified CVP Port Usage

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

* This is the default port. If you are using a different port, then the default port can be disabled.

Security Considerations

Note: Before commencing the installation, upgrade or maintenance process, the user carrying out this operation should be a domain user and have local administrator and SQL sysadmin privileges.

Mandatory Security Configuration

This section describes the steps you must take 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 or your installation may be vulnerable.

- You *must* configure **Secure Sockets Layer (HTTP)** for the Unified CCDM web application. For more information, see "Configuring SSL" on page 72.

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 "Disabling Anonymous Sessions" on page 31). 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 https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts-and-shares
- **Disable cached logins** on all Unified CCDM servers (see "Disabling Cached Logins" on page 32). 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 are unable to log in if the connection to the domain controller is unavailable. For more information, consult the Microsoft documentation https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-number-of-previous-logons-to-cache-in-case-domain-controller-is-not-available
- **Disable DCOM** on all Unified CCDM servers (see "Disabling DCOM" on page 32). 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 https://docs.microsoft.com/en-us/windows/desktop/com/setting-machine-wide-security-using-dcomcnfg#enabling-and-disabling-dcom
- **Enable mandatory Server Message Block (SMB)** signing (see "Enabling Mandatory SMB Signing for all Unified CCDM Servers" on page 33). 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 https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/smbv1-microsoft-network-server-digitally-sign-communications-always

Note: If you enable SMB signing, the server is not able to communicate with a Microsoft network client unless that client agrees to perform SMB packet signing. So SMB signing needs 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 "Disabling SSL V2" on page 33). 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.

3 Pre-Installation Tasks

- Configuring Windows
- Configuring User Accounts
- Installing and Configuring SQL Server
- Configuring Optional Security Settings

Configuring Windows

Configuring Firewalls

- If your installation requires it, configure the firewall ports as described in "Firewall Configurations" on page 22.

Configuring Settings on 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 **Remote Desktop 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 is unable to synchronize application data correctly between servers otherwise, and this may cause unexpected behavior.

Configuring User Accounts

Configuring Unified CCDM Service Accounts

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

Configuring Application Accounts

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

Configuring SQL Agent Users

- 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.

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 that 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.

> Note: For single-sided installations, you can choose to allow Unified CCDM to create these accounts automatically as local accounts. But if you choose this option, then you should add additional servers to your deployment later, and you need to reinstall the system.

To create the required accounts:

- 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**

Installing and Configuring SQL Server

Installing SQL Server on Dedicated Database Server

Follow these instructions to install SQL Server **2016** 64-bit Standard Edition on the server or servers hosting the database.

For a dual-sided deployment, perform these tasks on the Side A and Side B servers.

To install SQL 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. In the **Setup Role** window, select **Feature Installation**.
9. In the **Feature Selection** window, select the following instance features:
   - **Database Engine Services**
     - **SQL Server Replication**
   - **Shared Features**
     - **Client Tools Connectivity**
     - **Client Tools Backwards Compatibility**
10. Update the installation directories to the required locations. Click **Next**.

11. The installation rules are then checked. If any problems are reported, correct them, then click **Next**.
12. The Instance Configuration window is displayed. Select **Default Instance**, with an **Instance ID** of **MSSQLSERVER**. Update the Instance root directory to be installed on the required drive, then click **Next**.
13. 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**.
14. 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.
15. The Database Engine Configuration window is displayed. Set the following and click **Next**:
    a. Select **Mixed Mode authentication** and enter a password for the **sa** user.
    b. 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.
    c. Select the **Data Directories** tab. **Temp DB directory** and **Temp DB log directory** should not be located on the same drive as the Windows operating system. You may see a warning during Unified CCDM installation if they are. Make any required changes to the data directory locations.
16. You may see the Feature Configuration Rules window while installation checks are performed. If so, wait until the checks complete successfully.
17. Review the installation summary and click **Install**.
18. Once the installation is complete click **Close**.
19. When the SQL Server 2016 installation is complete, locate and install **SQL Server 2016 Service Pack 2**.

Installing SQL Server Management Studio (SSMS) Release 16.x or 17.x.

- Install SSMS 16.x or 17.x tool on the database server. For a dual sided deployment, perform these tasks on the Side A and Side B servers.

Configuring SQL Server Network Protocols

On the server or servers that host the Unified CCDM Database, configure the SQL Server network protocols listed in this section.

To configure SQL Server network protocols:

1. Launch **SQL Server 2016 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** to confirm.

4. In the right-hand pane, right-click on **TCP/IP**, select **Enable**, and click **OK** to confirm.
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.

Configuring Windows Firewall for SQL Server

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

To configure Windows firewall:

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 from becoming excessively large.
- Schedule backups for quiet times of the day.

Configuring Optional Security Settings

Disabling Anonymous Sessions

This step is optional, but must be done if you desire maximum security. See "Optional Security Configuration" on page 25 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.

To disable anonymous sessions:

1. In the Group Policy Editor, browse to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options** and enable the **Network access: Do not allow anonymous enumeration of SAM accounts and shares** setting.
2. Alternatively, you can update the registry directly by following these steps:
   a. In the **Run** command dialog box, enter **regedit**.
   b. In the **Registry Editor**, browse to select the **HKEY_LOCAL_ MACHINE > SYSTEM > CurrentControlSet > Control > Lsa** node.
   c. 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**.
   d. Close the **Registry Editor**.

Disabling Cached Logins

This step is optional, but must be done if you desire maximum security. See "Optional Security Configuration" on page 25 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.

To disable cached logins:

1. In the **Group Policy Editor**, browse to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options** and set the **Interactive logon: Number of previous logons to cache (in case domain controller is not available** setting to **0**.
2. Alternatively, you can update the registry directly by following these steps:
   a. In the **Run** command dialog box, enter **regedit**.
   b. In the **Registry Editor**, browse to select the **HKEY_LOCAL_ MACHINE > Software > Microsoft > Windows Nt > CurrentVersion > Winlogon** node.
   c. 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**.
   d. Close the **Registry Editor**.

Disabling DCOM

This step is optional, but must be done if you desire maximum security. See "Optional Security Configuration" on page 25 for more information.

This security setting applies to all Unified CCDM servers.

To disable DCOM:

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.

Enabling Mandatory SMB Signing for all Unified CCDM Servers

This step is optional, but must be done if you desire maximum security. See "Optional Security Configuration" on page 25 for more information.

This security setting applies to all Unified CCDM servers.

To enable mandatory SMB signing:

1. In the **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.
   a. Launch **Server Manager**.
   b. Click **Tools** select **Local Security Policy.**
   c. Navigate to **Local Policies > Security Options** and ensure that the following security options are set:
      - **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).

Disabling SSL V2

This step is optional, but must be done if you desire maximum security. See "Optional Security Configuration" on page 25 for more information.

Perform these tasks on each application/web servers.

To disable SSL V2:

1. In the **Run** command dialog box, enter **regedit**.
2. In the **Registry Editor**, browse to **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.

Disabling Remote Access to Unified CCDM Servers

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

4 Installation Process

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. Make sure to install the components in the order described here.

Recording Your Settings

During the installation procedure, there are occasions where you need to record what settings you chose for later reference. You should record the following information and store it in a secure location, for future reference.

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

About the Unified CCDM Installer

Verifying Signature File for ISO

To verify signature file for ISO:

1. Download and install **openssl** from https://slproweb.com/products/Win32OpenSSL.html

   Any type of installer (either EXE or MSI) with any bit (32 or 64) can be downloaded from the link.

2. Install the download **openssl** using the instructions provided on the website. Have the **openssl** path added to the system path environment variable so that **openssl** command can be launched from any path.

3. Place the ISO image, ISO image signature file, and the public key.der in the same folder.
   - **UCCDM.12.5.7292.3825.iso.signature**
   - **UCCDM.12.5.7292.3825.iso**
   - **UCCEReleaseCodeSign_pubkey.der**

4. Launch the command prompt by right-clicking and choosing **Run as administrator**.

5. Execute the **cli** command in the command prompt to verify the authenticity and integrity of the CCO downloaded ISO.

   Syntax: `Openssl dgst -sha512 -keyform der -verify` *<public Key.der>* `-signature` *<ISO image.iso.signature> <ISO Image>*

   For example: `Openssl dgst -sha512 -keyform der -verify UCCEReleaseCodeSign_pubkey.der -signature UCCDM.12.5.7292.3825.iso.signature UCCDM.12.5.7292.3825.iso`

6. Upon successful verification, output is **Verified OK** and on failure **Verification failed.**

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 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 can click **Install** to install the chosen component.

Installing the Database Components

Perform the following steps on the Side A Database server.

To install the database components:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see "About the Unified CCDM Installer" on page 37).
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. Click **Next** to go to the next window.
5. In the **License Agreement** window, you must accept the terms of the license agreement before proceeding. When you have read and agreed to the terms, click **Next.**
6. In the **Cryptography Configuration** window, provide the following and click **Next**:
   - **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 cannot be able to continue until the contents of this field are identical to the passphrase entered above.

Important: **The cryptographic passphrase is a vital piece of information and is 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 are unable to access your existing data.

7. In the **Configure Database** window, provide the following and click **Next**:
   - **SQL Server:** This field is greyed out and the value is set to `localhost`.
   - **Catalog 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**
  - **SQL Server authentication using the login ID 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.

8. 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. Click **Next**.
9. Click **Install** to install the database components. During this process, the **J2SE** prerequisite is 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.
10. 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**.

Note: If the Launch Database Management Utility check box is not checked, you can access Database Management Utility through the Database Installer.

11. Click **Finish**.

Installing the Portal Database

Note: The installation of the Portal Database fails 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 "Changing the SQL Server Installation Language to US English" on page 129.

To install the portal database:

1. If you selected the **Launch Database Management Utility** check box after installing the database components (page 39), the database setup wizard starts 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, provide the following and click **Next**:
   - **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 for Unified CCDM. You use the default name of **Portal**. This should match the database catalog name specified when you installed the database components. If not, you 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**
  - **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, the message **Connection succeeded but database does not exist** is displayed.

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 automatically split into 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, TempDB should not be installed on the same disk as the operating system.

   - **To split a file group**, choose the **Split** option, click the dropdown 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 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 dropdown 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 are 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 before clicking **Next**:
   - **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`.

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 before clicking **Next**:
   - 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.

Note: You may not wish to have the default static max size value that is automatically set for the Max Size field based on the analysis of your system. While setting "Unrestricted size is not recommended, auto-growth can be enabled to minimize the risk of Unified CCDM's SQL database into a state where you are not able to make changes.

   - To specify a different **Initial Size**, first clear **Set Initial Size** to **Max Size**.
   - To change default initial size limit of 15mb, select the **Set Initial Size** checkbox and set the new size.

- You can also choose an unlimited file size by selecting **Unrestricted Size**, but this does not guarantee optimal performance.
- Auto growth value is always set. This value is **Use to grow the size of filegroup**.
- 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.

Note: After the size of the database has been set, the system calculates the size of the **TempDB** and **TempDBLog**. The file sizes should be adjusted in accordance with the values in SSMS.

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

The folder path may not be the folder path where SQL Server is installed. The database installer places the database files on different drives, based on an algorithm that uses the space available on each of the server drives.

8. The **Configure Local Administrator Details** window sets the identity details for the default administrator account:
   - **Name:** The type of user account that is 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 cannot 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. Provide and verify the following before clicking **Next**:
   - **Account Type:** The type of user account that is 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 "Configuring Application Accounts" on page 28. If you used a different name when setting up the account, enter that name instead. If you have specified a domain user, you need to prefix the user name with the domain name, followed by a backslash. For example, if the SQL agent user belongs to the **ACMEDOM** 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 additional servers in future, you have 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 cannot continue until the contents of this field are identical to the password entered above.

10. In the **Configure the Location of the Identity Data Files** window, select the location of the identity data files.
    a. To change the location, click **Location**.
    b. Select the location of each file group.
    c. Click **OK** to save your changes.
    d. 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 takes several minutes

> Note: If the installation reports an error saying that the SQL Server language must be US English, you need to fix this before you can install the Portal Database. For instructions, "Changing the SQL Server Installation Language to US English" on page 129. Then repeat the installation of the Portal Database.

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

Installing the Application and Web Server

Install the new Application/Web Server components.

To install the application and web server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see "About the Unified CCDM Installer" on page 37).
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. Click **Next** to go through the installer.
4. If the **Domain Manager: Application Server Components Dialog** is shown, click **Next** to install the additional required components.
5. If the **Microsoft .NET 4.6.2 Framework** prerequisite is missing, it is installed at this point. Click **Install** to install the component and follow the on screen instructions. When the .NET 4.6.2 Framework is complete, restart the server to continue the installation of the Application/Web Server.
6. In the **License Agreement** window, you must accept the terms of the license agreement before proceeding. When you have read and agreed to the terms, click **Next.**
7. In the **Cryptography Configuration** window, provide the following details and click **Next**:
    - **Passphrase:** Enter the cryptographic passphrase you used for the installation of the Database Server component.

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

Important: **You must use the same cryptographic passphrase for all servers in the Unified CCDM installation. If you do not know the cryptographic passphrase, stop the installation immediately and contact your vendor support. If you continue the installation with a new passphrase the installation does not work.**

8. 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.
9. In the **Configure Database** window, provide the following details and click **Next**:
   - **SQL Server:** Enter the host name or IP Address of the server hosting the Unified CCDM database. 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 is **Portal**.
   - **Connect Using:** Select the login credentials you want to use:
     - **Windows authentication credential of application**
     - **SQL Server authentication using the login ID 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 a SQL Server Login Name and Password in the fields provided.

Important: **You must check that you have provided valid database credentials. There is no database validation check present when installing application server components.**

10. In the Ready to Install the program window, click **Install**.
11. When the installation has completed, click **Finish**. When installation is complete, a dialog box for restating the machine appears. Click **Yes** to restart the server now, or **No** to restart later.

Installing the Identity Server

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

To install the identity server:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see “About the Unified CCDM Installer” on page 37).
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 **Welcome to the Domain Manager: Identity Server setup wizard** window, click **Next**.

5. In the **End-User License Agreement** window, you must accept the terms of the license agreement before proceeding. When you have read and agreed to the terms, click **Next.**
6. In the **Configure Cryptography Configuration** window, provide the following details and click **Next**:
   - **Passphrase:** Enter the cryptographic passphrase you used for the installation of the Database Server component.
   - **Confirm Passphrase:** You cannot continue until the contents of this field are identical to the passphrase entered above.

Important: **You must use the same cryptographic passphrase for all servers in the Unified CCDM installation. If you do not know the cryptographic passphrase, stop the installation immediately and contact your vendor support. If you continue the installation with a new passphrase the installation does not work.**

7. In the **Destination Folder** window, click **Change...** to browse to the destination folder you want to install into.
8. In the **Ready to install Domain Manager: Identity Server** window, click **Install** to begin installation. Installation takes several minutes.
9. 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.

Important things to note:

- 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 cannot happen that quickly.
- If you are using a load balancer then the URL must be used in the Unified CCDM setup ICE wizard - the web server machine names should not be used. This means a load balancer needs to be setup before configuring Unified CCDM.
- When load balancing, only sticky connections are supported. User sessions can only use one web server.

This involves two steps:

- Share the same signing certificate (page 44)
- Ensure identity server affinity (page 45)

To 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**

Important: **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.**

Important: **Note that the Id Server signing certificate is different from the Application Server certificate.**

2. On **Side B**, import the signing certificated certificate. Update the identity server **web.config** (**D:\Program Files\Domain Manager\Identity Server\Identity.Server\web.config**) if a custom certificate is used. You need to give **NetworkService Read** permissions to the private key. To do this:
   - Click **Certificate**, and then **All Tasks**.
   - Select **Manage Private Keys**.

To 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.

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 www.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 correctly uses the Identity Server running on the same physical machine.

Installing the Second Side (Replicated Systems Only)

For replicated systems this installation needs to be repeated for Side B. You should complete the Side A installation of all components before installing Side B.

5 Unified CCDM Configuration

About Unified CCDM Configuration

This chapter describes how to configure the server cluster and perform data replication.

This section describes the following steps:

- Configuring the Unified CCDM cluster
- Configuring ADFS
- Configuring Unified CCE Admin Workstations
- Configuring Unified CCE for provisioning
- Configuring replication

Configuring 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*.

Starting ICE Cluster Configuration

For a dual-sided deployment, perform these tasks on the Side A and Side B servers.

To start ICE 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 is **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.

Configuring 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

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

To set up the Unified CCDM servers:

1. In the **ICE Cluster Configuration** tool, select the **Setup** tab and click **Setup Unified CCDM Servers** to start the wizard. Click **Next** to go through each window in turn.
2. On the **Select Deployment Type** page, choose **Two Tier deployment** type. Note that the **All in one** server installation is not supported.
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 value as 1 on each side of your deployment. Click **Next**.
5. On the **Configure Core Servers** pages, enter the server name and server address for each of the Unified CCDM servers.
6. On the **Configure Application Servers** page, provide the following details:
   - **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 depends on the method of access to the application website, based on whether it is with or without load balancer. With load balancer, the FQDN is the load balancer FQDN and must be specified in all **Configure Application Server** pages. Without load balancer, the FQDN is 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 cannot 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 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:** If this mode is selected, each Unified CCDM service connects 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 are prompted to create it.
11. The **Deployment Summary** page summarizes the choices you have made. Check the deployment details, and if you are satisfied, click **Next**.
12. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.
13. To save and action your changes, either click the **Save** icon in the tool bar or select **File > Save** from the menu.

Resetting System Administrator Password

You can use ICE to reset the system administrator password.

To reset the password:

1. In the **ICE Cluster Configuration** tool, select the Setup tab and click **Reset The Administrator Password.**
2. Enter the **New password** and **Confirm Password** and click **Next**.
3. A confirmation message is displayed to indicate that the password was set successfully. Click **Exit** to close the wizard.

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.

After making any changes to Unified CCE, you need to reconfigure Unified CCE using the **Configure Cisco Unified CCE Servers** Wizard.

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

Unified CCDM requires a connection to:

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

Configuring Cisco Unified CCE Servers

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

If you require resource management (provisioning), you 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>_<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.

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.
4. On the **Configure Redundancy** page, select whether you want to configure a single-sided or a dual-sided Unified CCE.
5. 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 Unified CCE, provide the corresponding server details for the Side B server.
6. On the **Configure Connection Details** page, enter the authentication details to connect to the Admin Workstation database.
   - **Windows Authentication:** This is the default 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.
7. On the **Select Unified CCE Instance** page, select the AW instance to be used in the deployment. Click **Next**.
8. On the **Select Required Components** page, select all the required components in the deployment.
   - **Admin Workstation:** This option is disabled and selected by default.
   - **Provisioning Components (ConAPI/Unified Config):** Select this component if you require resource management.
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 and only shown if you selected the **Provisioning Components (ConAPI/Unified Config)** option above), 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>**`_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. 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.
- **Command Timeout (seconds):** Set the command timeout for the server. It is set to 120 seconds by default.

Note: If the user permissions are changed then you need to start "Apache Tomcat" service on UCCE.

10. On the **Configure Primary ConAPI RMI Ports** page, (only shown if you selected the **Provisioning Components (ConAPI/Unified Config)** 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 is usually be **2099**.
    - **Remote Registry Port:** This is the port on the Unified CCDM Database Server for the Unified CCE to connect to. This is 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 Unified CCE (or specific server, for example, `AW`) and Unified CCDM server must be configured to allow both-way traffic on this port.

Note: If dual-sided UCCE is being configured, 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 **Provisioning Components (ConAPI/Unified Config)** 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 "Setting Up ConAPI" on page 65.
    - **Application Key:** Use the password for the application you specified above.
12. On the **Multi Media Support** page, select **Yes** to provide support for non-voice interactions. The default value 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 **Configure Active Directory Global Catalog Connections** page, provide the details of active directory global catalog and configure the security settings to connect.

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

15. The **Summary** page 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**.
16. A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.

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

Important notes about configuring Unified CCE servers:

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

The CMS server on each side of the Unified CCE instance requires there be a node for each side of the Unified CCDM system. That is:

- Side A of Unified CCE needs two nodes for Unified CCDM, Side A and Side B with the same Administration & Data Server RMI registry port and Application RMI registry port for both nodes.
- Side B of Unified CCE needs two nodes for Unified CCDM, Side A and Side B with the same Administration & Data Server RMI registry port and Application RMI registry port for both nodes but must be different to the Side A Unified CCE configured ports.

For example:

Servers:

- Unified CCDM Side A: UCCDMDB_A
- Unified CCDM Side B: UCCDMDB_B
- Unified CCE Instance Side A: ICMSIDE_A
- Unified CCE Instance Side B: ICMSIDE_B

On ICMSIDE_A the following CMS nodes are created:

1. Administration & Data Server Link: UCCDMDB_AServer
   - Administration & Data Server RMI Registry Port: 2099
   - Application Link: UCCDMDB_AClient
   - Application RMI registry port: 2099
   - Application host name: UCCDMDB_A
2. Administration & Data Server Link: UCCDMDB_BServer
   - Administration & Data Server RMI Registry Port: 2099
   - Application Link: UCCDMDB_BClient
   - Application RMI registry port: 2099
   - Application host name: UCCDMDB_B

On ICMSIDE_B the following CMS nodes are created:

1. Administration & Data Server Link: UCCDMDB_AServer
   - Administration & Data Server RMI Registry Port: 2098
   - Application Link: UCCDMDB_AClient
   - Application RMI registry port: 2098
   - Application host name: UCCDMDB_A
2. Administration & Data Server Link: UCCDMDB_BServer
   - Administration & Data Server RMI Registry Port: 2098

- Application Link: UCCDMDB_BClient
- Application RMI registry port: 2098
- Application host name: UCCDMDB_B

Configure Cisco Unified CVP Servers

This task is optional. It is only required if you are planning to use **Media File Management.**

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.
        - **Command Timeout (seconds):** Set the command timeout for the server. It is set to 120 seconds by default.
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 each of the remaining call servers.
10. On the **Configure Unified CCE Server** page, select the Unified CCE server that is linked to the Unified CVP Instance being configured. This is an optional step.
11. The **Summary** page summarizes the details of the Unified CVP cluster 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. To save and action your changes, either click the **Save** button in the toolbar or select **File > Save** from the menu.

Creating and Mapping 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

To create a Unified CCDM tenant:

1. In the **ICE Cluster Configuration** tool, select the **Equipment Mapping** tab. In the center pane, right-click 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 are prompted to save your changes when you exit the tool.

Creating Folders

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 are prompted to save your changes when you exit the tool.

Creating an Equipment Mapping

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

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 are 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 **Add** 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** dropdown list.
      - Peripheral

- Routing Client
- Media Routing Domain
- Remote Tenant

Select the specific item of that type that you want to map from the **Resource** dropdown 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:** Enables you to associate a specific active directory with a tenant or folder.
- **Small contact center settings:** Enables 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 Global Catalog Domain or Server 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 are 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 is created and provisioned, and any resources from the remote tenant that are associated with this department is imported into the selected folder or tenant.

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

If you want to use the customer resource mapping option, you cannot 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 are 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 are 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 are 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 are prompted to save your changes when you exit the tool.

Configuring 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.

Configuring ADFS Per Identity Server

Adding the Unified CCDM Identity Server to ADFS

To manually add the Unified CCDM identity server to ADFS:

1. Open **ADFS 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 **ADFS profile**, then click **Next**.
7. Click **Next**, as Unified CCDM does not support optional token encryption certificates.

8. Select **Enable support for the WS-Federation Passive protocol**, and enter the full URL of the identity server **ADFSendpoint**. The endpoint must be in the correct format. Endpoint should be: `https://fqdn/identity/adfs/logout`

Note: The URL must use an SSL certificate that ADFS trusts, and must be in the correct format. For example, `https://fqdn/Identity/adfs`.

9. Under **Relying party trust identifier**, enter the full URL of the identity server. The URL must be in the correct format. For example, `https://fqdn/Identity`. 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.

Editing Claim Rules for Unified CCDM

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**.

Note: You should use a System Identification Number (SID) as NameID, as it is necessary for the NameID to be unique to each user.

Claim Rule Name	Mandatory	Store	LDAP Attribute	Outgoing Claim Type
AD: SID as NameID	Yes	Active Directory	objectSid (type directly)	Name ID
AD: UPN as Name	Yes	Active Directory	User-Principal-Name	Name
AD: GivenName	No	Active Directory	Given-Name	Given-Name
AD: Surname	No	Active Directory	Surname	Surname
AD: Email	No	Active Directory	E-Mail-Addresses	E-Mail-Addresses

5. Once the claims have been setup, click **Finish** to close the dialog.
6. Alternatively, if you wish to support automatic user provisioning:

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

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

c. 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** to close the dialog.

Configuring 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.

Configuring ADFS

To configure ADFS as a one-time setup:

1. Open **ADFS 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:** `distinguishedname`
   - **Ongoing Claim Type:** `http://temp.org/claims/DistinguishedName`

   Select or type to add more.
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.

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

Mapping Tenants to ADFS

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

To map tenants to ADFS:

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.

Configuring 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.

Setting Up Administrator Account

To set up an administrator account:

1. Login to Unified CCDM as **administrator**.
2. Click the **Hamburger** icon and click on **Security** and then select **User**.
3. Click **New**.
4. Enter the following details to create a user account to be the new administrator account:
   - The login name must correspond to an existing Windows Active Directory user, and must be formatted as `<domain-name>\<username>`, 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.
   - Deselect the **Local Login Enabled** checkbox.
5. Click on the newly created user and open the Groups tab.

6. Click **Add to Group**.
7. Select the checkbox for the **Administrators** group.
8. Close and save.

Configuring Windows Authentication

To configure Windows authentication 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 is **Portal**.
   - **Authentication:** Select any authentication configured on the database.
2. Click **OK**. The ICE Cluster Configuration tool starts by default.
3. In the **Tools** dropdown, select **System Properties**. The System Properties tool is displayed. In **Enabled Login Types**, make sure that the **Windows** option is selected. It is required to setup the Windows authentication mode.
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 all the domain users have the parent folder path in the **Inherited from** column.

   If this is not set, or it is set to **NONE**, then click **Change Permissions**, select the user, and click the **Replace all child objects permissions entries with inheritable permission entries from the object** check box to grant explicit permission, and click **OK**.
8. Click **Yes** on the confirm window message.
9. Click **OK** to close the properties dialog.
10. From a command window, execute the **iisreset** command.

Note: The next step is only required if you have a custom web URL configured to access your Unified CCDM system.

11. 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-webservername>` 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
```

12. Reboot the Unified CCDM App/Web Server or servers.

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

13. 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 are 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.

Managing Users with Windows

Login names for new users should be in the **<domain-name>\<username>** 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*.

Configuring Unified CCE Admin Workstations

> Note: If Windows Authentication is used, then the service account needs appropriate permissions. If SQL Server Authentication is used, then SQL Server account needs appropriate permissions.

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

To configure Unified CCE Admin workstations:

1. Login to the AW as a user with local administrative privileges.
2. Launch **SQL Server Management Studio**. Connect to the server.
3. Open up the **Security** folder, and right-click **Logins**.
4. Select **New Login** from the dropdown list. The Login – New window displays.

5. Add SQL logins for the Network Service accounts of each server hosting Unified CCDM (Database Servers and App/Web Servers), by filling in the fields as follows:
   - **General** page:
     - **Login Name:** Enter the machine name in the form `<DOMAIN>\<MACHINENAME>$`, for example `ACMEDOM\ACMESERVERA$`. This configures access for the NETWORK SERVICE account from the Unified CCDM server.
     - **Authentication:** Select **Windows Authentication** unless connecting to a server on a different domain.
   - **User Mapping** page**:**
     - **Users mapped to this login:** Select **AWDB** and **HDSDB**.
     - **Database role membership for:** For **AWDB** and **HDSDB**, select **Public** and **db_datareader**.
6. Click **OK**.

Configuring 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.

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

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

Setting Up ConAPI

You must run the Configuration Manager on the Unified CCE Admin Workstation (AW) to set up ConAPI.

To set up the ConAPI application instance:

1. Open the 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, set the /admin switch in order to run Unified Communications Manager.

2. Under **Tools > List Tools,** double click the **Application Instance List** option 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.
   - **Description:** Provide application instance description. This is optional field.
4. Record these details for use during the configuration of the cluster.
5. Click **Save** and then click **Close**.

Setting Up the CMS Server

Checking CMS Server Set Up

Ensure that the CMS Servers are set up correctly on each Unified CCE.

To check CMS server setup:

1. 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.
2. 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.

Adding New Application Connection

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 add new application connection:

1. On the Unified CCE being configured, launch **CMS Control**. This opens the CMS control console.
2. Click **Add** 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:** Refer to the firewall port table for the relevant port numbers.
   - **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. 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**. Click **OK** again to cycle the **CMSJServer**, save your changes and close the CMS Control console.

Configuring 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 "Configuring Replication" on page 67.
- Monitor replication as described in "Monitoring the Replication Snapshot" on page 69.

For more information about using the ICE Replication Manager to manage replication at a later date, see the *Integrated Configuration Environment (ICE) Guide 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 on 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**
- **Identity Database – "[IdSvr3Config] : IDMerge"**

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 takes the longest for the snapshot process to complete. Each of the publications 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.

Configuring 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 "Configuring Replication" on page 66.

Configure Replication Share Folder

For a dual-sided system, the replication share folder must be reconfigured. Follow these steps on the Side B Database Server:

To configure replication share folder:

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, and give the **Everyone** group full control to the share, by following these steps:
   a. Right-click on the replication folder and select **Properties.**
   a. In the Properties window, go to the Sharing tab.
   b. On the Sharing tab, click the **Advanced Sharing** button.
   c. Select the **Share this folder** option and provide 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*. For more information, see **Step 6** of Installing the Portal Database.
   d. Now, click the **Permissions** button.
   e. In the Permissions window, select the group **Everyone**, and select the Allow check-box next to the **Full Control** option.
3. Click **OK** to apply the changes.

Configure Replication on Database Server

To configure replication on the Database Server that is 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 is **Portal**.
   - **Authentication:** Select **Windows Authentication**.
2. Click **OK**. The ICE Cluster Configuration tool starts by default.
3. From the **Tool** dropdown 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 is 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. To replicate the Identity Server Database, select the **Identity Database Replication Enabled** checkbox. This option is selected by default.
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 value should be **distribution_portal**.
   - **Data Folder:** The folder path on the distributor server where the data file for the distribution database is 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 is created.
   - **Distribution Share:** The distribution share folder where replication snapshot files are generated.
   - **Override Distributor Admin Password:** Select to override the auto-generated replication password which is used to establish connectivity. The auto-generated password is 14 characters long, and contains 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.

Monitoring 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:** Lists the publisher servers and the publications on each publisher that need to be shared with the subscribers.

- **Subscriptions and Agents:** 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:** Shows all sessions for the selected publication and replication agent in the last 24 hours.
- **Actions:** 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 starts with **[Portal]**.

   Wait for the replication snapshot for this publication to complete.

3. 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 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 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*.

6 Post-Installation Process

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

Configuring SSL

Follow the instructions in this section to configure SSL for the Unified CCDM web application. To configure SSL for Unified CCDM you need to:

- Obtain a digital certificate if you do not already have a suitable one. For more information, see "Obtaining a Digital Certificate" on page 72.
- Export the certificate in PFX format. For more information, see "Exporting the Certificate in PFX Format" on page 73
- Configure SSL for the Unified CCDM web application. For more information, see "Configuring SSL for the Web Application" on page 74.

Note: These steps are mandatory and some features of the web application do not work properly unless you do this.

These steps are also required if you are upgrading, even if you have already configured SSL for a previous version.

Obtaining 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: You should use a digital certificate with a key length of at least 2048 bits. Some recent browsers may reject certificates with shorter key lengths.

If you do not already have a suitable certificate, you can request or generate one.

To request an external certificate:

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 **Server Certificates**.
3. In the **Actions** pane, select **Create Certificate Request** to display the **Request Certificate** dialog box.

4. In the **Common Name** field, enter the application domain name. Take care to enter it exactly as specified here. The certificate does 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.domain.com`, enter `www.domain.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://domain.intranet.local`, enter `domain.intranet.local`.
   - For deployments where the web servers are accessed directly with no load-balancing, enter the fully qualified domain name of the server being configured. For example, `webserver1.mydomain.com`.
5. Complete the other fields as appropriate, and click **Next**.
6. In the **Cryptographic Service Provider Properties** dialog box leave the default Cryptographic Service Provider. Select a bit length of at least **2048**. Click **Next**.
7. Specify a file name for the certificate, and then click **Finish**.
8. 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**.
9. Enter the file name of the certificate, and a Friendly Name of your choice and click **OK**.

To generate an internal certificate:

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 **Server Certificates**.
3. In the Actions pane, select **Create Domain Certificate** to display the **Distinguished Name Properties** dialog box.
4. In the **Common Name** field, enter the application domain name. Take care to enter it exactly as specified here. The certificate does 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.domain.com`, enter `www.domain.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://domain.intranet.local`, enter `domain.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.`
5. Complete the other fields as appropriate, and click **Next**.
6. In the **Online Certification Authority** dialog box specify the **Online Authority** and a name. Click **Finish**.

Exporting 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 **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.

Configuring SSL for the Web Application

To configure SSL for the web application:

1. In a web browser, navigate to `http://` *<web-address>* `/SSLConfig`, where *<web-address>* is the web address of your Unified CCDM deployment. For example, if your web address is *http://domain.intranet.local*, enter `http://domain.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 the **Browse** or **Choose File** button and browse to the PFX file you created in the previous section.
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.`

Binding Server Ports to IPv6 Addresses

This is an optional task and needs to be performed only if IPv6 network is available. The server ports that are used for **http** and **https** communications must be bound to IPv6 addresses only.

To bind ports on the App/Web server:

1. In **IIS Manager**, expand the **Sites** node and select **Default;Web Site**.
2. Under **Actions**, select **Bindings**.
3. Select **http** and click **Edit**. In the IP Address field enter `[::1]`. Click **OK**.
4. 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.
5. Click **OK**, then **Close**.
6. At the command prompt, enter **iisreset**.

Configuring Antivirus Options

If you have antivirus software on the Unified CCDM servers, you should 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, do the following:
  a. Start **SQL Management Studio** and expand the **Databases** node.
  b. Select **Properties** for each of the databases in turn. If you selected the default database name at installation, the database is set as **Portal**.
  c. 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 is **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 ensure optimal performance of Unified CCDM.

Application/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 https://technet.microsoft.com/en-us/library/2007.09.utilityspotlight.aspx	
Set Windows audit policy settings to disable success audits for audit logon events. See: http://technet.microsoft.com/en-us/library/cc758201(v=ws.10).aspx for more information (link checked November 2014).	

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 https://technet.microsoft.com/en-us/library/2007.09.utilityspotlight.aspx	
Ensure the Portal database is set to **Simple Recovery Mode** on all systems.	

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 is at `C:\Program Files\DomainManager\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 **Unified CCDM: 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

Installing Microsoft KB Patches

- Before starting the Unified CCDM services, any necessary Microsoft KB patches must be installed. Ensure the Unified CCDM services are stopped and set to “disabled” before applying any Microsoft KB patches. Once all patches have been applied, re-enable the Unified CCDM services before restarting the system.

Enabling Registry Auditing

You can enable registry auditing to keep track of the changes made to the registry on the servers. This is an optional task.

To enable registry auditing:

1. In elevated mode, run the following command from Command Prompt:

   ```
   auditpol /set /subcategory:"Registry" /success:enable
   ```

   Note: If the Operating System has a different language pack, the name **Registry** might differ. For instance, on a German Windows Operating System, the name is **Registrierung**. To see the name of the subcategory, you can run the following command:

   ```
   auditpol /list /subcategory:*
   ```

2. Open Registry Editor and navigate to the key which we want to audit:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Exony`
3. Right-click the key and choose **Permissions…**
4. Click **Advanced** and switch to the Auditing tab.
5. Add a user or group (using 'Select a principal' if not already there)
6. Select **Type** as **All**.
7. Select **Applies to** as **This key and subkeys**.
8. Check **Full Control** under Basic permissions (or Advanced permission).
9. Click **OK.**
10. Apply settings.

Restarting the System

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

Logging in to Unified CCDM

To login to Unified CCDM

1. Launch the Unified CCDM application. This opens a web page, which you can bookmark.
2. To login to a new system, use the user name **administrator** and the password set during the database installation. If you are logging into an upgraded system, the administrator password is the same as before.

Verifying 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.

To verify the installation:

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. In the **ICE Service Manager** tool, verify that all the installed Unified CCDM Services are running.
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.

Checking Database Credentials

- Once the application server is installed and configured, you should check that you have provided a valid database credential.

  There is no database validation check present when installing application server components.

7 Upgrade Process

About the Upgrade Procedure

The following table lists the Unified CCDM versions you can upgrade from and the OS and SQL version changes that need to be considered while upgrading from previous versions.

Important things to note:

1. Single server deployments are not supported from version 11.5 onwards. If you have a single-server deployment on version 11.0, then in order to upgrade to 12.5 you need two VMs – one for Databases and one for app/web servers.
2. Version 12.0 and higher require Windows Server 2016 and SQL Server 2016 SP2. Earlier versions used Windows Server 2012 R2 and SQL Server 2014 SP2.
   - In-situ upgrades are not supported while upgrading from 11.6.1 or lower versions. You need to prepare new servers with Windows Server 2016 Operating System on all servers and SQL Server 2016 SP2 on database server for upgrade.
   - Upgrade from 12.0 to 12.5 is done in-place and does not require new servers.

Upgrade from	OS (Windows) version changes	SQL version changes	Rebuild VM?
▸ 11.0, 11.5, 11.6 to ▸ 12.5	▸ Windows Server 2012 R2 changes to ▸ Windows Server 2016	▸ SQL 2014 SP2 changes to ▸ SQL 2016, SP2	Yes
▸ 12.0 to ▸ 12.5	N/A	N/A	No

Upgrade Options

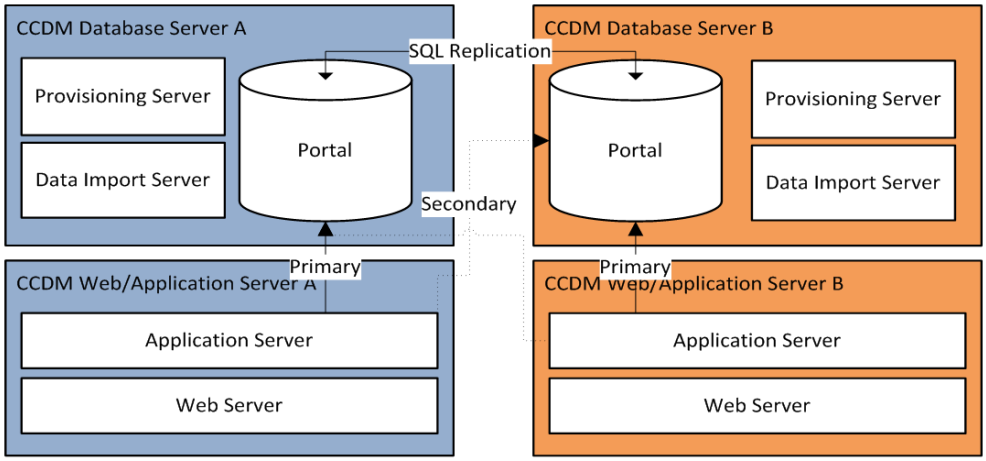
There are two upgrade options available - total outage upgrade and split-sided upgrade.

- **Single-sided** systems always use the **total outage upgrade** (page 84) option - where all systems are brought down and upgrade at the same time.
- For **dual-sided** systems you can do:
  - A **total outage upgrade** (page 84), when both A and B sides are turned off and upgraded at the same time.
  - A **split-sided upgrade** (page 103), when you turn off side A only and Side B is always available while upgrading the application to the latest version on the new servers.

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.



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 results 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.

Acquiring and Preparing New Windows 2016 Servers

> **Note:** Skip these tasks if you are upgrading from 12.0.1.

- Acquire new servers with Windows Server 2016. You must have these servers ready before you begin the upgrade process.
- These tasks need to be performed on the new Windows 2016 servers and do not require any downtime. Perform these tasks on both Side A and Side B servers.

Configuring New Windows Servers

- On the new Side A and Side B servers running Windows Server 2016, perform the Windows pre-installation tasks. See the "Configuring Windows" on page 28 section for details.

Creating User Accounts

- On the new Side A and Side B servers running Windows Server 2016, create the SQL Agent User account as described in "Configuring User Accounts" on page 28.

Configuring Optional Security Settings

- On the new Side A and Side B servers running Windows Server 2016, configure the security settings as described in "Configuring Optional Security Settings" on page 31.

Installing and Configuring SQL Server

- Install and configure SQL Server as described in "Installing and Configuring SQL Server" on page 29. Perform this task on the new Side A and Side B servers.

Upgrading Windows Server 2012 to Windows Server 2016 for Existing 12.0(1) Deployments

Before upgrading to 12.5(1), you must upgrade Windows Server 2012 to Windows Server 2016 on all 12.0(1) servers.

> Note: Perform these tasks on both Side A and Side B servers.

Downtime requirements: This upgrade requires a downtime as services is stopped on all servers when the operating system is being upgraded. While planning for downtime, take into account the time required to take VM backups and the time required to upgrade the operating system on all servers.

To upgrade Windows Server 2012 to Windows Server 2016 for existing 12.0(1) deployments:

1. Stop all the services of CCDM 12.0.1 Windows 2012 setup. See page 87 for instructions.
2. On all the CCDM servers, disable the CCDM services by changing the start type from **Automatic** to **Disabled** from the Services window.
3. Take a backup of all the VMs where CCDM components are installed. The VM must be shutdown before taking a backup.
4. On all the CCDM servers, update Windows Server 2012 R2 to Windows Server 2016.

5. On all the CCDM servers, enable the CCDM services by changing start type from **Disabled** to **Automatic** from the Services window.
6. Start all the CCDM 12.0(1) services. See page 100 for instructions.

8 Total Outage Upgrades

This chapter describes the steps involved to upgrade a single-sided and dual-sided deployment, where all servers is taken down and upgraded at once.

Important: **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 need it during the upgrade.

About Total Outage Upgrades

In a total outage upgrade all the servers are brought down and upgraded at the same time. Single-sided systems always use the total outage upgrade option. For dual sided systems, you can use a total outage upgrade option, where you bring down both side A and side B at the same time and upgrade both sides in one go. Optionally, you can use the split-sided upgrade option (page 104) for dual-sided systems.

Checklist for Total Outage Upgrades for Single-Sided and Dual-Sided Systems

Step	Complete
"Acquiring and Preparing New Windows 2016 Servers" on page 81 (Task to be performed outside the downtime) **Note:** This step is required only if you are upgrading from 11.6.1 or lower version.	
"Preparing to Upgrade" on page 87	
Updating Folder Names in Resource Manager	
Stop the Unified CCDM services	
Remove database replication (Only when upgrading dual-sided systems)	
Backup the Unified CCDM Portal Database	
Backup the Unified CCDM Identity Database (Only when upgrading from version 11.5, 11.6 or 12.0. Identity database is introduced in 11.5)	
Restore the Portal and Identity databases **Note:** This step is required only if you are upgrading from 11.6.1 or lower version.	

Step	Complete
Configure the SQL Agent User **Note:** This step is required only if you are upgrading from 11.6.1 or lower version.	
Add Network Service Accounts **Note:** This step is required only if you are upgrading from 11.6.1 or lower version.	
"Upgrading and Configuring Unified CCDM Components" on page 91	
Install the Database Components	
Upgrade the portal database	
Install Database Components and Upgrade portal database (Side B)	
Install the App/Web server	
Install the identity server	
Reconfigure the Unified CCDM servers	
Reconfigure the Unified CCE Servers	
"Reconfigure Unified CCE to Use the New Servers" on page 96	
"Restoring Replication" on page 97	
Configure Replication (Only when upgrading dual-sided systems)	
Monitor the replication snapshot (Only when upgrading dual-sided systems)	
"Post-Upgrade Tasks" on page 99	
Bind Server Ports to IPv6 Addresses **Note:** This step is required only if you are upgrading from 11.6.1 or lower version.	
Configure SSL	
Restart the System	
Log in to Unified CCDM	
Verify the installation	
Run user migration tool (Only when upgrading from version 11.0)	
Restart the Unified CCDM Services	
Validate the upgrade	

Preparing to Upgrade

Updating Folder Names in Resource Manager

- In Resource Manager, the following characters are not allowed in folder names: Space, Dot(.), tilde(~), hyphen (-), underscore(_), curly bracket {}, circle bracket(), hash (#), single quote (`). You must update the folder names before upgrading.

Stopping the Unified CCDM Services

Before starting the upgrade, perform the following steps on the Side A database servers to stop all Unified CCDM services running on both sides.

To stop the Unified CCDM Database Server services:

1. Launch the Integrated Configuration Environment (ICE) tool.
2. In the Database Connection window, provide the database connection details and click **OK**.
3. From the **Tool** dropdown, select **Service Manager**.
4. Select all the Unified CCDM Services and click **Stop Selected**.
5. A dialog box appears to state that all the services are stopped. Click **Close**.

Removing 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 is **Portal**.
   - **Authentication:** Select **Windows Authentication**.
3. Click **OK**. The ICE Cluster Configuration tool starts by default.
4. From the **Tool** dropdown 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.

Backing 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.

Perform the following steps on the Side A Database Server and then repeat the steps on the Side B Database Server.

To back up the Portal database:

1. Launch SQL Server Management.
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.

Backing up the Identity Database

Back up the Identity 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.

Perform the following steps on the Side A Database Server and then repeat the steps on the Side B Database Server.

Note: This step is only required when you are upgrading from Unified CCDM version 11.5 onward.

To back up the identity database:

1. Launch SQL Server Management.
2. Navigate to the Identity database.
3. Right-click **IdSvr3Config** and select **Tasks > Backup**. Save the `.bak` file to a suitable location.
4. Close SQL Server Management Studio.

Restoring the Portal and Identity Databases

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

Note: Skip this task if you are upgrading from 12.0.1.

To restore the databases:

On the Side A New 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 and identity databases backup to the Side B Database Server.

Configuring the SQL Agent User

For a dual-sided system, the SQL Agent User must be reconfigured. Perform the following steps on the Side A Database Server and then repeat the steps on the Side B Database Server.

Note: Skip this task if you are upgrading from 12.0.1.

To configure the SQL agent user:

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.

Adding 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.

Perform this task on Side A and Side B servers.

Note: Skip this task if you are upgrading from 12.0.1.

To add network service accounts:

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**.

   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 that the **Windows authentication** option is selected and enter the `NTAUTHORITY\NETWORK SERVICE` account for the Side A web server in the following format:`<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.
11. Click **OK**.
12. For deployments with multiple web servers, repeat step 5. to step 11. for each additional web server.

Upgrading and Configuring Unified CCDM Components

Installing the Database Components

Perform the following steps on the Side A Database Server. If you are upgrading from 12.0.1 then perform the following steps on the existing Side A Database Server. This step needs to be performed on new Side A database server if upgrading from 11.6.1 or lower version.

To install the database components:

1. Insert the Unified CCDM DVD and start the Unified CCDM Installer (for more information about the Unified CCDM Installer, see "About the Unified CCDM Installer" on page 37).
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.
6. In the **License Agreement** window, you must accept the terms of the license agreement before proceeding. When you have read and agreed to the terms, click **Next.**
7. In the **Cryptography Configuration** window, provide the following:
   - **Passphrase:** Enter the cryptographic passphrase you created during the installation of the Database Server component when you first installed Unified CCDM. Note that you cannot access your existing data if you continue the installation with a new passphrase.
   - **Confirm Passphrase:** You will not be able to continue until the contents of this field are identical to the passphrase entered above.
8. In the Configure Database window, provide the following and click **Next**:
   - **SQL Server:** This field is grayed out and the value is set to `localhost`.
   - **Catalog Name:** Enter the name of the database catalog for Unified CCDM. By default this is **Portal**.
   - **Connect Using:** Select one of the following login credentials you want to use:
     - **Windows authentication credentials of application**
     - **SQL Server authentication using the login ID 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.
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. In Ready to Install the Program window 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.

Note: If the Launch Database Management Utility check box is not checked, you can access Database Management Utility through the Database Installer.

12. Click **Finish**.

Upgrading the Portal Database

Perform the following steps on the Side A Database Server. If you are upgrading from 12.0.1 then perform the following steps on the existing Side A Database Server. This step needs to be performed on new Side A database server if upgrading from 11.6.1 or lower version.

Note that the Identity Database is automatically upgraded along with the Portal Database.

To upgrade the portal database:

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 **Select An action to Perform** window choose **Upgrade an existing database**. Click **Next** to continue.
4. In the **SQL Server Connection Details** window, provide the following and click **Next**:
   - **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 I use to logon to my computer**
     - **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 **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**. A warning message may appear notifying about unpartitioned old audit data. Click **Yes** to clear the data now, or click **No** to continue the database upgrade as normal.

5. In the Ready to upgrade the database window, 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.

Installing Database Components and Upgrading Portal Database (Side B)

Perform the following steps on the new Side B Database Server. If you are upgrading from 12.0.1 then perform the following steps on the existing Side B Database Server. This step needs to be performed on new Side B database server if upgrading from 11.6.1 or lower version.

To install database components and upgrade the portal database on Side B:

1. Install the database components as described in "Installing the Database Components" on page 91.
2. Upgrade the Portal database as described in "Upgrading the Portal Database" on page 92.

Installing the Application/Web Server

Perform this task on the Side A App/Web Server and then repeat the steps on the Side B App/Web Server. If you are upgrading from 12.0.1, then perform the steps on the existing servers. This step needs to be performed on new servers if upgrading from 11.6.1 or lower version.

- Follow all steps in the section "Installing the Application and Web Server" on page 42.

Installing the Identity Server

Perform this task on the Side A App/Web Server and then repeat the steps on the Side B App/Web Server. If you are upgrading from 12.0.1, then perform the steps on the existing servers. This step needs to be performed on new servers if upgrading from 11.6.1 or lower version.

- Follow all steps in the section "Installing the Identity Server" on page 43.

Reconfiguring the Unified CCDM Servers

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. These steps do not need to be repeated on the Side B Database Server as the necessary changes are applied 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 is **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 **Select Deployment Type** page, choose **Two Tier deployment** type. Note that the **All in one** server installation is not supported.
5. On the **Configure Redundancy** page, select whether you would like to configure a single-sided or a dual-sided system. Click **Next**.
6. 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.
     - **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.
   - **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**.
8. Click **Next** to go through the remaining windows in turn, without changing anything.
9. When you see the confirmation message indicating that the wizard has completed successfully, click **Exit** to close the wizard.
10. To save your changes, either click the **Save** icon in the toolbar or select **File > Save** from the menu.
11. 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**.
12. To save and action your changes, either click the **Save** icon in the toolbar or select **File > Save** from the menu. Exit ICE.

Reconfiguring the Unified CCE Servers

Note: Skip this task if you are upgrading from 12.0.1.

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 as 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 is updated when replication is reinstated.

To reconfigure the Unified CCE servers:

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 is **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 is usually 2099.
   - **Remote Registry Port:** This is the port on the Unified CCDM Database Server for the Unified CCE to connect to. This is usually 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 Unified CCE 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 "Setting Up ConAPI" on page 65.
- **Application Key:** Use the password for the application you specified above.

8. On the **Multi Media Support** page, select **Yes** to provide support for non-voice interactions. The default value 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 **Configure Active Directory Global Catalog Connections** page, provide the details of active directory global catalog and configure the security settings to connect.

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

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 toolbar 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 reconfigure Unified CCE to use new servers:

Do this task 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 new Unified CCDM Database Server, in upper case, 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 upper case, 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 the CMS Control console.

   Repeat these steps on each Unified CCE instance in your Side B deployment.

Restoring Replication

Note: Before you start restoring replication, ensure that all the Unified CCDM services are in stopped state.

Configuring 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 is the Side A Database Server, but 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 is **Portal**.
   - **Authentication:** Select **Windows Authentication**.
2. Click **OK**. The ICE Cluster Configuration tool starts by default.
3. From the **Tool** dropdown 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 are 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. To replicate the Identity Server Database, select the **Identity Database Replication Enabled** checkbox. This option is selected by default.
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 name is commonly **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. This does not apply for in-place upgrades.

   - **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 is used to establish connectivity. The auto-generated password is 14 characters long, and contains 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.

Monitoring 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** lists the publisher servers and the publications on each publisher that need to be shared with the subscribers.
   - **Subscriptions and Agents** 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** shows all sessions for the selected publication and replication agent in the last 24 hours.
   - **Actions** 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 starts 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 Tasks

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

- Configure HTTPS as described in "Configuring SSL" on page 72.
- Bind server ports to IPv6 addresses as described in "Binding Server Ports to IPv6 Addresses" on page 74

- Complete the final post-installation actions described in "Final Post-Installation Actions" on page 77.

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 "Configuring Windows Login" on page 61.

Running User Migration Tool

Note: You need to run this tool only when you are upgrading from version 11.0 to version 12.5.

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.

Restarting the Unified CCDM Services

Following an upgrade it is a 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.

To restart the Unified CCDM services:

1. Launch the Integrated Configuration Environment (ICE) tool.
2. In the Database Connection window, provide the database connection details and click **OK**.
3. From the **Tool** dropdown, select **Service Manager**.
4. Select all the Unified UCCDM Services and click **Start Selected**.
5. A dialog box appears to state that all the services are started. Click **Close**.

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.

Validating the 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.
Log in the application on Side A and create a new Precision Queue. This tests provisioning from the Side A App/Web Server. Run this test against each configured Unified CCE instance.	The Precision Queue should be created successfully and 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.

Check	Success Criteria
CVP Media file upload	
Log in to the web application on Side A and create a new Media file. This test provisioning from the Side A App/Web Server and will test the working of CVP media upload. Run this test against each configured Unified CCE instance.	The media file should be uploaded successfully and visible in the CVP servers.

9 Split-Side Upgrades

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 disconnects the replication and communication channels between the two sides of the system, so each side can operate independently as a single-sided 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.

Do not make any Unified CCDM specific changes during the upgrade. Limit changes to provisioning and re-skilling on Unified CCE during the upgrade as the same will be replicated once the upgrade is done.

This process has two parts.

- **Part 1:** Split the dual-sided system and upgrade Side A (see "Checklist for Split-Sided Upgrades (Side A)" on page 104).
- **Part 2:** Upgrade Side B and restore replication (see "Checklist for Split Side Upgrades (Side B)" on page 111).

The description assumes that you have a two-tier deployment (separate Database and Application/Web servers).

Important: **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-Sided Upgrades (Side A)

The first part of the split-side upgrade splits the dual-sided system and upgrades Side A.

Step	Complete
Acquiring and Preparing New Windows 2016 Servers on page 81 (Task to be performed outside the downtime) **Note:** This step is required only if you are upgrading from 11.6.1 or lower version.	
"Preparing to Upgrade" on page 105	
Updating Folder Names in Resource Manager	

Step	Complete
Stop the Unified CCDM services for Side A and Side B	
Remove database replication	
Start the Unified CCDM services for Side B on existing servers	
Backup the Unified CCDM Portal Database from Side B Database Server	
Backup the Unified CCDM Identity Database from Side B Database Server (Only when upgrading from version 11.5 or 11.6. Identity database is introduced in 11.5)	
Update Side B to enable provisioning and import	
Restore the Portal and Identity databases on new Side A Database Server **Note:** This step is required only if you are upgrading from 11.6.1 or lower version.	
Configure the SQL Agent user (Side A) **Note:** This step is required only if you are upgrading from 11.6.1 or lower version.	
Add network service accounts (Side A) **Note:** This step is required only if you are upgrading from 11.6.1 or lower version.	
"Upgrading and Configuring Unified CCDM Components (Side A)" on page 110	
Install the Database Components	
Upgrade the portal database	
Install the App/Web Server	
Install the Identity Server	

Preparing to Upgrade

Refer to this section about the necessary preparation steps when preparing to upgrade Side A.

Updating Folder Names in Resource Manager

- In Resource Manager, the following characters are not allowed in folder names: Space, Dot (.), tilde (~), hyphen (-), underscore (_), curly bracket {}, circle bracket (), hash (#), and single quote (`). You must update the folder names before upgrading.

Stopping the Unified CCDM Services (For Side A and B)

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

To stop the services on the Database Server:

1. Launch the Integrated Configuration Environment (ICE) tool.
2. In the Database Connection window, provide the database connection details and click **OK**.
3. From the **Tool** dropdown, select **Service Manager**.
4. Select all the Unified CCDM Services of Side A and B and click **Stop Selected**.
5. A dialog box appears to state that all the services are stopped. Click **Close**.

Removing 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 is **Portal**.
   - **Authentication:** Select **Windows Authentication**.
3. Click **OK**. The ICE Cluster Configuration tool starts by default.
4. From the **Tool** dropdown 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.

Updating Side B to Enable Provisioning and Importing

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 update Side B to enable provisioning and importing:

- Follow the steps described in the "Database Server Component Failover" section of 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.

Starting the Unified CCDM Services (Side B)

Start the Unified CCDM Services of Side B.

Note: At this point Side B on old servers is available for use.

To start the services on the Database Server:

1. Launch the Integrated Configuration Environment (ICE) tool from Side B database Server.
2. In the Database Connection window, provide the database connection details and click **OK**.
3. From the **Tool** dropdown, select **Service Manager**.
4. Select all the Unified UCCDM Services of Side B and click **Start Selected**.
5. A dialog box appears to state that all the services are started. Click **Close**.

Backing up the Portal Database (Side A)

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:

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.

Backing up the Identity Database (Side A)

Back up the Identity 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.

Note: This step is only required when you are upgrading from Unified CCDM version 11.5 onward.

To back up the identity database:

1. Launch SQL Server Management.
2. Navigate to the Identity database.
3. Right-click the Identity database (**IdSvr3Config**) and select **Tasks > Backup**. Save the `.bak` file to a suitable location.
4. Close SQL Server Management Studio.

Restoring the Portal and Identity Databases (Side A)

Note: Skip this task if you are upgrading from 12.0.1.

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

Note: Perform this task on the new servers prepared for Side A.

To restore the databases:

On the Side A New 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.

Configuring the SQL Agent User (Side A)

Note: Skip this task if you are upgrading from 12.0.1.

The SQL Agent User must be reconfigured on the new server for dual-sided system.

Note: Perform this task on the new servers prepared for Side A.

To configure the SQL agent user:

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.

Adding Network Service Accounts (Side A)

Note: Skip this task if you are upgrading from 12.0.1.

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.

Note: Perform this task on the new servers prepared for Side A.

To add network service accounts:

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**.

   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 `NTAUTHORITY\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.
11. Click **OK**.
12. For deployments with multiple web servers, repeat step 5. to step 11. for each additional web server.

Upgrading and Configuring Unified CCDM Components (Side A)

Installing the Database Components

Note: If you are upgrading from 12.0.1, then perform these on the existing servers. This step will need to be performed on new servers if upgrading from 11.6.1 or lower version.

- Follow all steps in the section "Installing the Database Components" on page 38.

Upgrading the Portal Database

Note that the Identity Database is automatically upgraded along with the Portal Database.

To upgrade the portal database:

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 **Select An action to Perform** window choose **Upgrade an Existing Database**. Click **Next** to continue.
4. In the **SQL Server Connection Details** window, take provide the following:
   - **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 I use to logon to my computer**
     - **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**. A warning message may appear notifying about unpartitioned old audit data. Click **Yes** to clear the data now, or click **No** to continue the database upgrade as normal.
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.

Installing the Application/Web Server

Perform this task on the Side A App/Web Server. If you are upgrading from 12.0.1, then perform the steps on the existing servers. This step will need to be performed on new servers if upgrading from 11.6.1 or lower version.

- Follow all steps in the section "Installing the Application and Web Server" on page 42.

Installing the Identity Server

Perform this task on the Side A App/Web Server. If you are upgrading from 12.0.1, then perform the steps on the existing servers. This step needs to be performed on new servers if upgrading from 11.6.1 or lower version.

- Follow all steps in the section "Installing the Identity Server" on page 43.

Checklist for Split Side Upgrades (Side B)

The second part of the split side upgrade applies the upgrade to Side B and restores replication. Many of the steps used in upgrading Side A apply to Side B. Unless otherwise noted, refer to the preparation steps for Side A for each of the sections that follow.

Step	Complete
Acquiring and Preparing New Windows 2016 Servers on page 81 (Task to be performed outside the downtime) **Note:** This step is required only if you are upgrading from 11.6.1 or lower version.	
"Preparing to Upgrade (Side B)" on page 112	
Backup the Unified CCDM Portal Database	
Backup the Unified CCDM Identity Database	
Restore the Upgraded Side A Portal and Identity Databases	
Configure the SQL Agent user **Note:** This step is required only if you are upgrading from 11.6.1 or lower version.	
Add network service accounts **Note:** This step is required only if you are upgrading from 11.6.1 or lower version.	
"Upgrading and Configuring Unified CCDM Components (Side B)" on page 114	
Install the Database Components	
Install the App/Web Server	
Install the identity server	

Step	Complete
Reconfigure the Unified CCDM servers	
Reconfigure the Unified CCE Servers	
"Restoring Replication" on page 118	
Configure Replication	
Monitor the replication snapshot	
"Post-Upgrade Tasks" on page 120	
Bind Server Ports to IPv6 Addresses	
Configure SSL	
Restart the system	
Log in to Unified CCDM	
Verify the Installation	
Run User Migration Tool (Only when upgrading from version 11.0)	
Restart the Unified CCDM Services	
Validate the upgrade	
Stop the Unified CCDM Services on old Side B servers	

Preparing to Upgrade (Side B)

Backing up the Upgraded Side A Portal Database

Back up the upgraded Side A 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 selected database server:

- Follow the steps outlined in "Backing up the Portal Database (Side A)" on page 107. You must back up the upgraded Side A database.

Backing up the Upgraded Side A Identity Database

Back up the upgraded Side A 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.

Note: This step is only required when you are upgrading from Unified CCDM version 11.5 onward.

- Follow the steps outlined in "Backing up the Identity Database (Side A)" on page 107.

Restoring the Upgraded Side A Portal and Identity Databases (Side B)

Restore the upgraded Side A portal (page 112) and Identity (page 112) database from the Side A back-up you made earlier.

Note: If you are upgrading from 12.0.1, then perform the steps on the existing servers. This step needs to be performed on new servers if upgrading from 11.6.1 or lower version.

To restore the databases:

On the Side B New 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 restores 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.

Configuring the SQL Agent User (Side B)

Note: Skip this task if you are upgrading from 12.0.1.

To configure the SQL agent user:

On the Side B Database Server, follow the steps outlined in "Configuring the SQL Agent User (Side A)" on page 108. Perform this task on the new servers prepared for Side B.

Adding Network Service Accounts (Side B)

Note: Skip this task if you are upgrading from 12.0.1.

- Follow the steps outlined in "Adding Network Service Accounts (Side A)" on page 109. Perform this task on the new servers prepared for Side B.

Upgrading and Configuring Unified CCDM Components (Side B)

Installing the Database Components (Side B)

To install the database components on the Side B Database Server:

Perform this task on the Side B database server. If you are upgrading from 12.0.1, then perform the steps on the existing servers. This step will needs to be performed on new servers if upgrading from 11.6.1 or lower version.

- On the Side B Database Server, follow the steps outlined in "Installing the Database Components" on page 110.

Installing the Application/Web Server (Side B)

To install the Application/Web Server:

Perform this task on the Side B App/Web Server. If you are upgrading from 12.0.1, then perform the steps on the existing servers. This step needs to be performed on new servers if upgrading from 11.6.1 or lower version.

- Follow the steps outlined in "Installing the Application and Web Server" on page 42.

Installing the Identity Server (Side B)

Perform this task on the Side B App/Web Server. If you are upgrading from 12.0.1, then perform the steps on the existing servers. This step needs to be performed on new servers if upgrading from 11.6.1 or lower version.

- Follow all steps in the section "Installing the Identity Server" on page 43.

Reconfiguring 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. These steps do not need to be repeated on the Side B Database Server as the necessary changes are applied when replication is reinstated.

To update the cluster configuration:

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 is **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.

Reconfiguring 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 as 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:

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 is **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 Unified CCE 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 "Setting Up ConAPI" on page 65.
   - **Application Key:** Use the password for the application you specified above.

8. On the **Multi Media Support** page, select **Yes** to provide support for non-voice interactions. The default value 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 **Configure Active Directory Global Catalog Connections** page, provide the details of active directory global catalog and configure the security settings to connect.

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

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 toolbar or select **File > Save** from the menu.

Reconfigure Unified CCE to Use the New Servers

Note: Skip this task if you are upgrading from 12.0.1.

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 reconfigure Unified CCE to use new servers:

Do this task 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 new Unified CCDM Database Server, in upper case, 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 upper case, 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 the CMS Control console.

Restoring Replication

Note: Before you start restoring replication, ensure that all the Unified CCDM services are in stopped state.

Configuring 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:

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 is **Portal**.
   - **Authentication:** Select **Windows Authentication**.
2. Click **OK**. The ICE Cluster Configuration tool starts by default.
3. From the Tool dropdown 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. To replicate the Identity Server Database, select the **Identity Database Replication Enabled** checkbox. This option is selected by default.
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 value should be **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. This does not apply for in-place upgrades.

   - **Log Folder:** The folder path on the distributor server where the transaction log file for the distribution database is created.
   - **Distribution Share:** The distribution share folder where replication snapshot files are 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 contains 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.

Monitoring 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 Tasks

After you have upgraded Unified CCDM, complete the following post-installation steps on both Side A and Side B servers:

- Configure HTTPS as described in “Configuring SSL” on page 72.
- Bind server ports to IPv6 addresses as described in “Binding Server Ports to IPv6 Addresses” on page 74

- Complete the final post-installation actions described in "Final Post-Installation Actions" on page 77.

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 "Configuring Windows" on page 28.

Running User Migration Tool

Note: You need to run this tool only when you are upgrading from version 11.0 to version 12.0.

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.

Restarting the Unified CCDM Services

Following an upgrade, you should restart all Unified CCDM services.

Perform the following steps on the Side A database servers to restart all Unified CCDM services running on both side.

To restart the Unified CCDM services:

1. Launch the Integrated Configuration Environment (ICE) tool.
2. In the Database Connection window, provide the database connection details and click **OK**.
3. From the **Tool** dropdown, select **Service Manager**.
4. Select all the Unified CCDM Services and click **Start Selected**.
5. A dialog box appears to state that all the services are started. Click **Close**.

Validating the Upgrade (Side A and Side B)

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

This step needs to be performed from both sides to validate that application is working fine from Side A and B.

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.
Log in the application on Side A and create a new Precision Queue. This tests provisioning from the Side A App/Web Server. Run this test against each configured Unified CCE instance.	The Precision Queue should be created successfully and 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.
CVP Media file upload	
Log in to the web application on Side A and create a new Media file. This test provisioning from the Side A App/Web Server and will test the working of CVP media upload. Run this test against each configured Unified CCE instance.	The media file should be uploaded successfully and visible in the CVP servers.

Stopping the Unified CCDM Services

Note: Skip this task if you are upgrading from 12.0.1.

After the new Side A and Side B servers are ready for use, stop the services on the old Side B servers.

To stop the Unified CCDM Database Server services on Side B:

1. Launch the Integrated Configuration Environment (ICE) tool.
2. In the Database Connection window, provide the database connection details and click **OK**.
3. From the **Tool** dropdown, select **Service Manager**.
4. Select all the Unified CCDM Services and click **Stop Selected**.
5. A dialog box appears to state that all the services are stopped. Click **Close**.

10 Uninstalling Unified CCDM

This chapter describes how to remove the Unified CCDM components from the platform.

Uninstallation involves the following steps:

- Removing Database Replication on page 125 (dual-sided systems only)
- Uninstalling Identity Component on page 126 (Identity component must be uninstalled before the Application Server component)
- Uninstalling Application Server Component on page 126
- Uninstalling the Database Component on page 126
- Removing the Database Catalog on page 127 (only if Unified CCDM is being removed permanently)

Removing 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:

- Ensure that the database is in a consistent state.
- 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 is **Portal**.
   - **Authentication:** Select **Windows Authentication.**
3. Click **OK**. The **ICE Cluster Configuration** tool starts by default.
4. From the **Tool** dropdown 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.

Uninstalling Identity Component

In a dual-sided deployment, perform the following steps on the Side A Application/Web server and then repeat the steps on the Side B Application/Web server. The Identity component must be uninstalled before the Application Server component.

To uninstall the identity server components:

1. On the Side A App/Web Server, launch Control Panel and select **Programs and Features.**
2. Select **Domain Manager: Identity Server**.
3. Click **Uninstall**.
4. 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 Application Server Component

The Identity component must be uninstalled before the Application Server component.

To uninstall the application server 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.
5. 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 Component

In a dual-sided deployment, perform the following steps on the Side A Database Server and then repeat the steps on the Side B Database Server.

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. 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.

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

Removing the Database Catalog

This permanently removes the database catalog.

Important: **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's support.**

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

To remove the database catalog for portal database:

1. Launch SQL Server 2016 Management Studio and connect to the local Database Server.
2. In the **Object Explorer** pane, expand the **Databases** node, navigate to the Portal 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.

To remove the database catalog for identity server database:

1. Launch SQL Server 2016 Management Studio and connect to the local Database Server.
2. In the **Object Explorer** pane, expand the **Databases** node, navigate to the Identity Server database (name is **IdSvr3Config**), 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.

11 Troubleshooting Tasks

- About Installer Logs
- Changing the SQL Server Installation Language to US English
- Portal Login Error Messages

About Installer Logs

- Unified CCDM installers are launched with logging enabled. Install logs are located in **C:\InstallLogs** for both the Database and Application/Web Server installers.

Changing the SQL Server Installation Language to US English

If the step to install the portal database fails with the following error, you must change the SQL Server language to US English before the installation can continue.

```
Exception in installation: [SQL Server language must be US English]
```

To do this, on the database server, run the following T-SQL scripts in the specified order.

On the database server, run the following T-SQL scripts in the specified order.

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
```

In Script 3, *<username>* is the Windows domain user or the SQL Server user you will specify for the **Connect Using** option during the installation of the Portal Database (in the SQL Server Connection Details window (page 39)).

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>*.

Portal Login Error Messages

Symptom: Error Message Appears Upon Logging into Portal Webpage

An error is displayed upon logging on to the Portal Webpage and the Identify Server logs show the following:

```
Date-Time INFO [14 ] Logging.TraceSourceSink User is not authenticated.
Redirecting to login.

Date-Time INFO [14 ] Logging.TraceSourceSink End authorize request

Date-Time INFO [14 ] Logging.TraceSourceSink Redirecting to login page

Date-Time INFO [11 ] Logging.TraceSourceSink Login page requested

Date-Time INFO [14 ] Logging.TraceSourceSink rendering login page

Date-Time INFO [11 ] Logging.TraceSourceSink Login page submitted

Date-Time ERROR [9 ] Logging.TraceSourceSink Unhandled exception accessing:
/Identity/login

System.Data.SqlClient.SqlException (0x80131904): The EXECUTE permission was
denied on the object 'ap_adm01_create_new_session', database 'Portal', schema
'dbo'.
```

Cause

The portalapp role was not added to the Web server Network Service account for the Portal database during the installation.

Recommended Actions

1. Launch SQL Server Management Studio.
2. In the Object Explorer, expand the Portal database. A list of folders is displayed.
3. Expand the **Portal > Security > Users** folder. A list of database logins is displayed.
4. Open the *DOMAIN**WEBSERVER MACHINE NAME*$ account.
5. In the **Select a page** pane, click **User Mapping**.
6. In the **Users mapped to this login** section, select the Portal database.
7. Ensure that the User column correctly contains the Network Service account for the Web server.

8. In the **Database Role Membership** section, select the portalapp role.
9. Click **OK**.
10. For deployments with multiple web servers, repeat for each additional Web server.