Installation Guide for Cisco Unified Contact Center Management Portal

Release 7.5(1)

July 2008

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

1. Unified Contact Center Management Portal ..............................8
   Overview .........................................................................................................8
   Primary Functionality ..................................................................................8
   Deployment Specifics ...................................................................................9
   Deployment Models .....................................................................................10
   N-Sided Replication ................................................................................ 10

2. Installation Guidelines and Requirements ..........................11
   Installation Prerequisite Checklist .............................................................11
   Database .......................................................................................................11
   Application ...................................................................................................11
   Web ..............................................................................................................12
   Data Import ..................................................................................................12
   General Advice .............................................................................................12
   Server Requirements ..................................................................................12
   Windows ......................................................................................................12
   SQL Server ..................................................................................................13
   Backup Guidelines ......................................................................................14
   Security Guidelines .....................................................................................14
   Reporting Services Security Configuration ............................................. 14
   Required User Accounts .............................................................................15
   sql_agent_user ........................................................................................15
   NT AUTHORITY\NETWORK SERVICE ................................................... 15

3. Component Installation ...............................................................16
   Planning Your Installation ..........................................................................16
   Recording Your Settings ............................................................................16
   Component Installation ...............................................................................17
   Database Component ..................................................................................17
   Database Component Installation ...........................................................17
   Database Setup ..........................................................................................18
   Database Replication ............................................................................... 20
   Application Server Component ..................................................................20
Application Server Component Installation ................................................ 20

**Web Server Component** ................................................................. 21
  Web Server Component Installation ............................................. 22

**Data Import Server Component** .................................................. 22
  Data Import Server Component Installation ................................... 22

**Product Documentation** ................................................................. 23
  Documentation Installation ........................................................... 23

**SysMon** ........................................................................................... 23

4. **Component Configuration** ......................................................... 24

**Data Replication** ........................................................................... 24
  Configuring the SQLSERVERAGENT Service .................................. 24

**Platform Server Cluster Configuration** ......................................... 25
  Configuration Overview ............................................................... 25
  Common ConAPI Credentials ....................................................... 25
  CMS Server Setup ........................................................................ 26
  Configuration Procedure .............................................................. 27

**CVP Media File Upload** .................................................................. 36
  Preparing the Configuration ......................................................... 36
  Configuring DFS for CVP Media File Upload .................................. 36
  Configuring DFS Root Targets ...................................................... 37
  Configuring File Replication for CVP Media File Upload ................. 37

**Performance Configuration Checklists** ......................................... 38
  Web Server .................................................................................. 38
  Database Server ........................................................................ 40

5. **Post Installation Steps** ................................................................. 41

  Logging into the Management Portal .............................................. 41
  Report Uploading ........................................................................ 41

6. **Upgrading From a Previous Version** ........................................... 42

  Overview ....................................................................................... 42

  Uninstalling the Portal ................................................................. 42
    Uninstalling Data Import Server Component ............................... 42
    Uninstalling the Provisioning Server Component ......................... 43
    Uninstalling Other Components .................................................. 43

  Upgrading SQL Server ................................................................. 44
    Upgrading to SQL Server 2005 Enterprise Edition ....................... 44
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrading to SQL Server 2005 Standard Edition</td>
<td>44</td>
</tr>
<tr>
<td>Installing the Portal</td>
<td>48</td>
</tr>
<tr>
<td>Configuration</td>
<td>48</td>
</tr>
<tr>
<td>Configuration Manager</td>
<td>48</td>
</tr>
<tr>
<td>Setting up ReportServer Connections</td>
<td>49</td>
</tr>
<tr>
<td>Replication</td>
<td>49</td>
</tr>
<tr>
<td>7. Platform Uninstallation</td>
<td>50</td>
</tr>
<tr>
<td>Uninstalling Data Import Server Component</td>
<td>50</td>
</tr>
<tr>
<td>Removing Replication</td>
<td>50</td>
</tr>
<tr>
<td>Uninstalling Data Import Server Component</td>
<td>50</td>
</tr>
<tr>
<td>Uninstalling the Database Component</td>
<td>51</td>
</tr>
<tr>
<td>Uninstalling All Other Components</td>
<td>51</td>
</tr>
<tr>
<td>8. Glossary</td>
<td>52</td>
</tr>
<tr>
<td>9. Index</td>
<td>58</td>
</tr>
</tbody>
</table>
PREFACE

Purpose
This document explains how to install the Unified Contact Center Management Portal components.

Audience
This document is intended for System Administrators with knowledge of their IPCC system architecture. SQL Server Database Administration skills are also an advantage.

Organization
Chapter 1, “Unified Contact Center Management Portal”
Introduces the Unified Contact Center Management Portal, including its integration with IPCC Enterprise and Hosted Editions, and how the Management Portal adds value to the system. It discusses how the Unified Contact Center Management Portal is used to configure (commission) a system deployment and manage that system.

Chapter 2, “Installation Guidelines”
Lists the prerequisites for the Unified Contact Center Management Portal installation and provides recommendations for pre-installation platform configuration, including platform and back up servers, antivirus software, security accounts, monitoring, system management and data replication between servers.

Chapter 3, “Component Installation”
Provides instructions for the installation of all the Management Portal components.

Chapter 4, “Component Configuration”
Describes post-installation configuration of the Unified Contact Center Management Portal, including setting up replication and uploading .wav files for voice announcements. The procedure for configuring a Unified Contact Center Management Portal server cluster is detailed as well as how to use the Cluster Configuration Manager to replicate data between Database servers. Web and Database component server performance checklists are also provided.

Chapter 5, “Post Installation Steps”
Describes how to set the administrator password for, and upload report templates into, the Unified Contact Center Management Portal platform.
Chapter 6, “Upgrading From a Previous Version”

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

Chapter 7, “Component Uninstallation”

Describes how to remove the Unified Contact Center Management Portal platform from your servers.

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

1. UNIFIED CONTACT CENTER MANAGEMENT PORTAL

Overview

The Unified Contact Center Management Portal is a suite of components that form part of the Cisco IPCC Enterprise and Hosted Editions. The Unified Contact Center Management Portal serves three mutually supportive purposes:

- It simplifies the operations and procedures for performing basic tasks such as adding or modifying Agents, Skill Groups, Teams and other common administrative functions.
- It provides a common web user interface to the product set. Currently, IPCC Enterprise and Hosted Editions and CallManager use different interfaces. Simple tasks therefore require performing multiple tasks in multiple applications to achieve a single goal such as adding an agent. By providing a web-based unified interface for common administrative tasks, the Cisco Unified Contact Center Management Portal decreases the amount of time, knowledge, training and resources currently required to administer the solution set.
- It provides an audit trail for changes made through IPCC. Through the supplied audit reports, or the individual resource histories, administrators and other power users can trace the timing and responsibility of provisioning changes.

IPCC Enterprise and Hosted Edition customers can optionally include the Unified Contact Center Management Portal to satisfy particular business requirements.

Primary Functionality

- **Unified Configuration**, that is, provisioning of the applicable IPCC components through a single task-based web interface.
- **Hierarchical Administration**, for example:
  - The Service Provider Administrator can add a Portal User
  - The Tenant Administrator can add a Skill Group
  - The Tenant Supervisor can add an Agent

  These permissions are completely configurable.
- **Audit Trails** on configuration changes and usage.

In terms of configuration, the Unified Contact Center Management Portal differentiates between commissioning and provisioning.

- **Commissioning** consists of operations that install and initially configure a system of components. These operations are typically done
by the Service Provider using existing setup and configuration tools. An example operation might be setting up and configuring a peripheral.

- **Provisioning** consists of day to day configuration operations performed by a tenant. Examples include creating or modifying Agents, Skill Groups and Agent Teams.

The Service Provider uses the existing IPCC, CallManager and CVP tools (installers and configuration tools) to commission a system. They will then install the Unified Contact Center Management Portal Provisioning System and use it to define organizational units and set up permissions. Units may then use the Unified Contact Center Management Portal Provisioning System to provision their specific site.

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

Additionally, the Unified Contact Center Management Portal system can read existing configuration data from IPCC Enterprise or Hosted Editions and CallManager, store it in the Unified Contact Center Management Portal database and reconcile differences between the two. This enables Service Providers to make configuration changes using existing IPCC and CallManager tools. These changes are automatically propagated into the Unified Contact Center Management Portal system.

**Deployment Specifics**

Unified Contact Center Management Portal platform deployments are limited to standard IPCC Enterprise and Hosted Edition, or System IPCC, deployments with the following restrictions:

- Each Tenant must have its own:
  - ICM or CICM instance
  - Dedicated Admin Workstation Real Time Distributor server. Multiple Distributor instances on a single server are not allowed
  - Dedicated Admin Workstation CMS Server. Multiple CMS Server instances on a single server are not allowed

- The Unified Contact Center Management Portal is only supported on IPCC Enterprise and Hosted Editions 7.1 and above, and System IPCC 7.5 and above.
Deployment Models

N-Sided Replication

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

Since the Unified Contact Center Management Portal scales up with equipment and scales out with servers, a variety of cost-effective deployment models are possible. Cisco recommends you read the Bill of Materials carefully prior to deployment model selection.

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

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

- **Secure Deployment.** The Unified Contact Center Management Portal Application, Web and Reporting components are hosted on one server and the Provisioning, Data Import and Database components are hosted on a second server. This system can manage 600 Portal users concurrently.
2. INSTALLATION GUIDELINES AND REQUIREMENTS.

Installation Prerequisite Checklist

Each Unified Contact Center Management Portal component requires prerequisite software installed in order to operate correctly. A mandatory check is performed before each part of the installation. If this check does not find the required software then the installation will refuse to proceed.

It is recommended that you install the prerequisites on the appropriate servers prior to starting any part of the installation.

A summary of these prerequisites is listed below.

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

Database
- Windows Installer 3.1
- Windows Server 2003 SP2
- Microsoft .NET Framework 2.0
- Microsoft SQL Server 2005 Standard or Enterprise Edition
- Microsoft SQL Server 2005 SP2 including Workstation Components

Application
- Windows Installer 3.1
- Windows Server 2003 SP2
- Microsoft .NET Framework 2.0
- Microsoft SQL Server 2005 SP2 Reporting Services Components

Web
- Windows Installer 3.1
- Windows Server 2003 SP2
- Microsoft .NET Framework 2.0
- Microsoft WSE 2.0 SP3
- ASP .NET State Service 2.0 enabled
- Microsoft ASP.NET 2.0 AJAX Extensions 1.0
- Unified Contact Center Management Portal: Application Component
Data Import

- Windows Installer 3.1
- J2SE Runtime Environment 5.0 (update 14)
- Microsoft .NET Framework 2.0
- Java 1.6.0.60
- Unified Contact Center Management Portal: Database Component (with database set up)

General Advice

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

Note: IE 6 SP2 is not available for Windows 2000, so any machine running this version of Windows will need to have IE 7 or later installed

Server Requirements

- Both the Portal servers and the IPCC servers should be configured to use the US English character set
- Install Windows 2003 Service Pack 2 on all the servers hosting the Unified Contact Center Management Portal
- Install all the latest Service Packs for: Windows 2003 (Service Pack 2), SQL Server 2005 (Service Pack 2) and Microsoft .NET v2
- Harden the Internet Information Services Web Server (IIS) and SQL Server 2005 according to Microsoft's latest guidelines
- Disable all unnecessary local services (FTP, BITS and so on)
- Use Microsoft Terminal Services for remote configuration and support

Windows

- Once the operating system and service pack have been installed, configure the Windows 2003 Application Server components as follows:
- Open the **Configure your Server Wizard**
- In the **Event Viewer**, set the **Application Log**, **Security Log** and **System Log** to **Overwrite events as needed**
- The following windows components are required:
  - **Microsoft Windows 2003 Application Server with ASP.NET components (IIS)** These must be selected as part of the application server configuration
  - **Microsoft .NET Framework 2.0** This is required on all servers
  - **Microsoft Script Host** Installed by default as part of Windows 2003

### SQL Server
- When installing the SQL Server database application, Cisco recommends that you accept the default settings
- Do not install SQL Server as a **named instance**
- Install SQL Server using **mixed-mode authentication** and use **local system** for the SQL Server and SQL Agent startup accounts
- Allocate SQL Server no more than 70% of the RAM in the server. Do not use dynamic RAM allocation
- Check the **Reporting Services** option during the Component Install section of the SQL setup
- Configure Reporting Services as follows:
  - **Report Server Virtual Directory** Create the report server virtual directory (the default of “ReportServer” is recommended)
  - **Report Manager Virtual Directory** Create the report manager virtual directory (the default of “Reports” is recommended)
  - **Windows Service Identity** Ensure that the report server service runs under the “Local System” account.
  - **Web Service Identity** Create a new application pool for the report server and manager to run in
  - **Database Connection** Create the report server database. This can be located on a different server
  - **Initialization** Ensure that your report server is initialized
  - **Email Settings** You will need to configure your email server here to allow users to schedule reports for delivery by email in the Portal
  - **Execution account** Set up an execution account to use for loading any external images that you may have in your reports
Backup Guidelines

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

Security Guidelines

- The Unified Contact Center Management Portal is usually deployed in an internet facing environment. Therefore plan security carefully before proceeding with the installation
- The platform follows a standard web deployment model, in which web servers are deployed in a demilitarized zone (DMZ). If security is particularly important, the database servers can also be deployed in their own DMZ
- The application should be installed while logged in using a domain account with administrative privileges over all of the platform machines
- When installing components that require a SQL Server Database connection you will be requested to select either Windows Authentication or SQL Server Authentication. Data access will be achieved using the built-in NETWORK SERVICE account if Windows Authentication is selected

Reporting Services Security Configuration

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

1. In Internet Explorer, open the Report Manager virtual directory on the Side A Web Application server. By default this is http://localhost/reports
2. Click on Site Settings from the menu at top right
3. Under the Security heading, click on the Configure site-wide security link
4. Click on New Role Assignment
5. Enter the NT AUTHORITY\NETWORK SERVICE user
6. Check System Administrator and click OK
7. Click Home to return to the main Report Manager page
8. Click the Properties tab
9. Edit the NT AUTHORITY\NETWORK SERVICE account
10. Check all roles and click Apply

Repeat this procedure for the network service accounts of all the Web Application servers. These accounts are of the form <domain name>\<machine name>$, for example CCMPDOM\WEBAPP2$.
Note If accessing localhost/reports shows the header only, this may mean that anonymous access on the Reports and Reportserver virtual directories is enabled. This should be disabled in IIS before continuing.

Required User Accounts

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

- Password never expires
- User cannot change password

sql_agent_user

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

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

NT AUTHORITY\NETWORK SERVICE

This account was created automatically by SQL Server 2000, but must be created manually when using SQL Server 2005.

1. Go to Start > All Programs > Microsoft SQL Server > Management Studio
2. Connect to Analysis Services
3. Right-click on the Analysis Server (this will be identified by the legend Microsoft Analysis Server 9.00.XXXX…) and select Properties
4. On the left side of the dialog box, in the Select a page pane, click on Security
5. If the NT AUTHORITY\NETWORK SERVICE account does not exist then click on Add to add the account
6. Under the Server Roles tab check the box for the following roles:
   - securityadmin
   - setupadmin
   - bulkadmin
7. Save and close
3. COMPONENT INSTALLATION

Planning Your Installation

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

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

The Cisco Security Agent (CSA) is disabled during the installation process.

Recording Your Settings

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

<table>
<thead>
<tr>
<th>Management Portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Catalog Name</td>
</tr>
<tr>
<td>sql_agent_user Password</td>
</tr>
<tr>
<td>portal_user Password</td>
</tr>
<tr>
<td>Cryptographical Passphrase</td>
</tr>
<tr>
<td>Administrator Password</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CICM/ICM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
</tr>
<tr>
<td>Application Key</td>
</tr>
<tr>
<td>Local Registry Port</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
</tr>
<tr>
<td>Application Key</td>
</tr>
<tr>
<td>Local Registry Port</td>
</tr>
</tbody>
</table>

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

**Component Installation**

1. Insert the Management Portal CD. A window consisting of a main panel and a number of tabs, corresponding to the Management Portal components, is shown

   **Note** If autorun is disabled, and you have not been presented with the Unified Contact Center Management Portal Products Installation Application, double click the `autorun.bat` file to launch the Unified Contact Center Management Portal installer.

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

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

4. To begin the installation of each individual component, click on its tab and click the **Run Test** button to check that the listed prerequisite applications are installed. Only when the installer has verified the presence of these components will you be able to click the **Install** button to proceed with the installation of that component

   **Note** Any prerequisite application that is not installed is displayed with a red cross next to it. These must be installed before the installation of the selected component can proceed. Once all the prerequisite software is installed click the **Re-Run Test** button to enable the **Install** button.

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

**Database Component**

This section details how to install the Unified Contact Center Management Portal Database server components.

**Database Component Installation**

To install the Unified Contact Center Management Portal Database component, perform the following:

1. Select the Database Component tab, click **Run Test** to check for prerequisites (see page 17), and click **Install**. Click **Next** to go through each window in turn

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

3. On the **Cryptography Configuration** dialog window:
1. **Passphrase** Create a cryptographical pass phrase of between 6 and 35 characters. This passphrase is used for encrypting and decrypting system passwords and must be the same for all servers in the cluster.

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

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

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

4. On the **Destination Folder** window, you can click the **Change…** button to change the location that the Database Server component is installed to.

5. Click **Install**

**Note** This does not install a new database component; it installs the database installation tool, which will be used to set up the database.

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

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

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

**Database Setup**

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

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

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

1. On the **SQL Server Connection Details** dialog window:
   - **Server Name** Select the SQL Server where the Unified Contact Center Management Portal database should be installed. In most cases this will be the machine running the application, in which case it should be left as the default (local).
   - **Database Name** Enter or select the name of the database catalog that will be used for Unified Contact Center Management Portal. It is recommended that you use the default name of **Portal**.
- **Connect Using** Select the radio button of the login credentials you wish to apply:
  - The Windows account information I use to logon to my computer This is the recommended option
  - The SQL Server login information assigned by the system administrator This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your Login Name and Password in the fields provided
- **Test Connection** Makes sure the connection to the SQL Server is established. The message ‘Connection succeeded but database does not exist’ is correct behavior at this point. Click OK to continue

2. On the **Select an Action to Perform** dialog window:
   - **Install a new database** Installs a new database. You may maintain or delete a database by running the installer again and selecting the appropriate option

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

4. The fields on the **Configure the Location of Data Files** dialog window only need to be completed if you are using a custom installation of SQL Server. If you are not using a custom installation of SQL Server, ignore these fields
   - **Location** When you select a File Group(s), its location is shown in this field. To change this location, browse to the new location
   - **Initial Size** Select the space that should be allocated for this File Group(s). The default is based on the Portal’s analysis of your system
   - **Max Size** Set the storage capacity for the selected File Group(s). You can also choose to set no limit to the file size by selecting the Unrestricted Size checkbox, though this is not recommended
   - **Update** Saves your changes to the selected File Group(s)
   - **Default** Returns the settings for all File Groups to their default

5. The **Configure SQL Server Agent Service Identity** window sets up a user account that is used by SQL Server for replication:
Account Type  The type of user account that will be used. For a distributed installation, this must be Domain.

User Name  The name of the user account. This defaults to sql_agent_user. If you used a different name when setting up the account, enter that name instead.

Automatically create the user account if missing  For a single sided system, it is possible to create the required user automatically. For all other systems, you must set up the required account manually. If you have not already created the user account, set it up now before continuing.

Password  Create a password for the new user, conforming to your individual system’s complexity requirements.

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

6. On the Web Application Servers Network Service Configuration window, enter the details of each Web Server to be used in the installation:

   - Domain  The network domain the web server is on, for example UCCMPPDOM
   - Machine Name  The name of the machine, for example WEBSERVERA

7. Click Add to add each Web Server to the list.
8. When all Web Servers have been added, click Next to begin installation. Installation will take several minutes.
9. Click Close to close the installer.

Database Replication

For replicated systems this installation will need to be repeated for side B. We recommend that a complete side A installation of all components is complete before installing side B.

Details on how to perform Database replication can be found in the Component Configuration chapter (Chapter 4).

Application Server Component

This chapter details how to install and configure the Unified Contact Center Management Portal Application Server components.

Application Server Component Installation

To install the Unified Contact Center Management Portal Application Server component, select the Application Server Component tab, click Run Test... to check for prerequisites (see page 17), and click Install.

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

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

2. On the **Destination Folder** window, you can click the **Change…** button to change the location that the Application Server component is installed to.

3. On the **Cryptography Configuration** dialog window:
   - **Passphrase** Enter the Cryptographical Passphrase chosen when installing the Database component.
   - **Confirm Passphrase** You will not be able to continue until the contents of this field are identical to the passphrase entered above.

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

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

4. On the **Cluster Configuration Database Connection** dialog window:
   - **SQL Server** Enter the name of the server where the Portal database has been installed.

**Note** The default value of the local machine is valid only for a standalone system.

   - **Catalog Name** Enter the name of the database, as selected in the Database Component installation (see page 18). By default this is Portal.

   - **Connect Using Windows authentication** should be used in most cases. If the database server is on a different network, select **SQL Server authentication** and enter the appropriate Login ID and Password in the fields provided.

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

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

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

**Web Server Component**

This section details how to install and configure the Unified Contact Center Management Portal Web Server component.
Web Server Component Installation

To install the Unified Contact Center Management Portal Web Server component, select the Web Server Component tab, click Run Test... to check for prerequisites (see page 17), and click Install.

Go through each step in turn. As you go, you will need to enter the following details:

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

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

3. When the installation is completed, click Finish

Data Import Server Component

Data Import Server Component Installation

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

To install the Unified Contact Center Management Portal Data Import Server component, select the Data Import Server Component tab, click Run Test... to check for prerequisites (see page 17), and click Install.

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

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

2. On the Cryptography Configuration dialog window:
   - Passphrase Enter the cryptographical passphrase you created during installation of the Database Server component
   - Confirm Passphrase You will not be able to continue until the contents of this field are identical to the passphrase entered above

Caution Do not dispose of the cryptographical pass phrase after installing the Data Import server component. The pass phrase should be securely recorded as it will be needed during installation of the Management Portal on new or replacement servers, and for upgrades. You will not be able to perform any of these tasks without it.

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

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

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

6. Click **Install**

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

**Product Documentation**

The Unified Contact Center Management Portal is delivered with all the documentation you need to install, configure and use it.

**Documentation Installation**

Open the Unified Contact Center Management Portal CD.
Select each manual and copy it to your preferred location.

**SysMon**

The Management Portal is delivered with a system monitoring tool designed to help monitor important properties of the Portal servers.

To install SysMon, select the SysMon tab, click Run Test… to check for prerequisites (see page 17), and click **Install**.

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

1. On the Select Installation Folder window:
   - Select a folder to install SysMon to. By default this is C:\Program Files\Management Portal
   - If you do not wish SysMon to be available to any user logged onto the machine, select the **Just me** radio button

2. Click **Install**

3. When the installation is complete, click **Close**

For information on configuring and using SysMon, see the **Administration Guide**.
Large enterprise-wide deployments may require multiple servers to host the Unified Contact Center Management Portal platform for reasons of performance or data security. Multiple platform hosts are connected together as a server cluster. This chapter details how to configure the server cluster and perform data replication. Performance tuning checklists are also provided for the Web and Database components.

### Data Replication

#### Configuring the SQLSERVERAGENT Service

The Management Portal installer automatically grants the sql_agent_user account the necessary permissions to log on as the SQLSERVERAGENT service, but it is still necessary to manually create folder shares and check access.

To do this:

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

The Cluster Configuration Manager is used to replicate data between Unified Contact Center Management Portal master and slave databases, which are called the Publisher and Subscriber databases respectively.

Before data replication between Unified Contact Center Management Portal databases can be performed, the server(s) in the cluster must first be setup with all the required prerequisite software and Unified Contact Center Management Portal components. Once prepared the servers need to be assigned publisher or distributor (subscriber) roles. See Portal Databases on page 28.

Now log back onto both machines as the domain administrator (or as the user who installed the Management Portal if this was not the domain administrator).

You are now prepared to set up replication as part of cluster configuration.
Platform Server Cluster Configuration

The Unified Contact Center Management Portal is normally hosted on multiple servers to improve performance and data security. The platform hosts are connected together as a server cluster. This section details how to configure the Unified Contact Center Management Portal server cluster and data replication.

The Portal’s Configuration Manager is an application that is used to configure server clusters, consisting of the Portal servers, Cisco ICMs and CallManagers that the Portal connects to. It is also used to set up replication between multiple Unified Contact Center Management Portal databases.

Configuration Overview

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

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

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

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

- The **Portal Server(s)** – the details of the server(s) containing the Unified Contact Center Management Portal database(s).
- The **NAM(s)** (relevant for IPCC Hosted Edition only) – the details of the server(s) hosting NAM(s) and the database credentials for accessing their data.
- The **CICM** or **ICM** – the details of the server(s) hosting the ICM and the database credentials for accessing their data.
- The **CallManager(s)** – the details of the server(s) hosting the CallManager, the endpoint and security credentials for accessing the AXL interface.

Common ConAPI Credentials

For each CICM (Hosted Edition) or ICM (Enterprise Edition) an application instance to connect through ConAPI needs to be set up. This is used by the Unified Contact Center Management Portal when making provisioning requests to add, update or delete items. You can use an existing application instance or create a new one.

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

To create an application instance, you must run Cisco Configuration Manager on the CICM or ICM server as follows:

1. Open the Configuration Manager. This can normally be done from **Start > Program Files > ICM Admin Workstation > Configuration Manager**

**Note** If you are connecting to the CICM/ICM server using Remote Desktop, you will need to set the `/console` switch in order to run the Configuration Manager.

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

3. Click the **Retrieve** button to display the list of configured application instances. To create a new application instance, click **Add**, and enter the following details:
   - **Name** A unique name to be used for the application instance
   - **Application Key** A password to be used by the Portal to connect. This may be between 1 and 32 characters
   - **Confirm Application Key** Ensure that no typographical errors were made while choosing the application key
   - **Application Type** Select **Cisco Voice**
   - **Permission Level** Give the application **Full read/write** permissions

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

5. Click **OK**

**CMS Server Setup**

Before configuring the Unified Contact Center Management Portal server cluster you must ensure that the CMS Server(s) are set up correctly on each CICM/ICM/NAM AW.

**Note** Each CICM/ICM requires a separate Admin Workstation running a single instance of CMS server

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

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

A new application connection must be defined on each configured CICM or ICM for each Data Import Server. This ensures that in a dual-sided system, the alternate side can also connect to the ICM in a failover scenario. To do this:
1. Go to **Start > Program Files > ICM Admin Workstation > CMS Control** on the CICM or ICM being configured. This opens the CMS control console.

2. Click on the **Add** button to the right hand side of the window to launch the **Application Connection Details** dialog window and fill in the fields as follows:
   - **ICM Distributor AW link** This should be the name of the Data Import server, all in capital letters, with ‘Server’ appended, such as UCCMPServer
   - **ICM Distributor AW RMI registry port** This is the port on the CICM for the Data Import server to connect to. This will usually be 2099, however if the Data Import server is connecting to multiple ICMs each should use a different port
   - **Application link** This should be the name of the Data Import server, all in capital letters, with ‘Client’ appended, such as UCCMPClient
   - **Application RMI registry port** This is the port on the Database Server for the CICM to connect to. For convenience, this should be the same as for the ICM Distributor AW RMI registry port. Each CICM must connect to a different port on the Database Server. You should record this information for future use.

**Note** Each CICM that the Portal will be provisioning must use a unique port on the Database Server.
   - **Application host name** The server name or fixed IP address, such as UCCMP or 240.24.53.107
   - Click **OK**, and **OK** again to save your changes and close the CMS control console.

**Configuration Procedure**

To configure the Unified Contact Center Management Portal server cluster proceed as follows:

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

2. The **Connect to SQL Server** dialog window is displayed. On this window:
   - **Server Name** This option defaults to the current machine and cannot be changed.
   - **Database** Select the Management Portal database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
   - **Use Integrated Security** Ensure this option is checked.

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

4. Enter the settings as described in detail below

5. Click **Save** to save your settings, or **Revert** to cancel your changes.
Note: When using integrated security, the user running the Configuration Manager application must have permission to execute SQL on the database server on which the application is running.

The window displays the following buttons. Click on a button to display the relevant configuration options.

1. Physical servers

This tab contains a list of all the servers in the cluster. Before a server is configured for a specific role such as NAM (IPCC Hosted Edition Only), or ICM it must be configured here.

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

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

- **Server Name** Enter the name of the server, such as UCCMPA
- **Default Hostname** Enter the hostname of the machine. This is the unique name by which it is known on the network, and may or may not be the same as the **Server Name**. The machine should be accessible using this host name from anywhere in the cluster.

Note: The Default Hostname cannot be an IP address.

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

2. Click OK.

The above steps should be repeated for all Unified Contact Center Management Portal Servers, ICM Servers, CallManager Servers and NAM Servers (IPCC Hosted Edition only) in this installation.

2. UCCMP Servers

Application Servers

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

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

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

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

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

Portal Databases

This tab is used to configure the relational databases.

1. Click the **Portal Databases** tab. A table is displayed, with four columns, that will display information about the Databases once they have been configured.
2. To add a new portal database server click **New**. The **Portal Database Configuration** dialog window is displayed.

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

3. Enter the following details:
   - **Server** Select the server that the database is installed on from the drop down list of the servers you configured on the **Servers** tab earlier. This defaults to the current machine.
   - **Catalog** Enter the name of the database in the field provided. This defaults to **Portal**.
   - **Default Database Connection Parameters** Select the radio button of the login credentials you wish the Database server to use:
     - **Windows authentication** Select this option only if the Local System user has administrator permissions on the server the CICM is installed on, or if you have configured the Data Import Server service to run under a different user that does have administrator permissions.
     - **SQL Server authentication** Most installations should select this option. Enter the **Login Name** and **Password** in the fields provided.

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

4. Click **OK**.

Once the publisher database has been set up, you can configure replication. It is recommended that replication be configured before CallManagers and either NAMs and CICMs, or ICMs are added to the cluster.

**Replication**

1. Click the **Replication** button. The **Cisco Database Replication Configuration** dialog window is displayed, in which all the selected server details are displayed. Perform any modifications at this stage if necessary.

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

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

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

5. Now log onto the Subscriber and open the **SQL Server Management Studio**, then open the **Replication Monitor**. Under **Agents/Snapshot Agents** three snapshot agents are listed.

6. Start the first snapshot agent (that for the **Base** publication) by right clicking on the agent and selecting **Start Agent**. Wait for the snapshot
status to change to ‘succeeded’ (this may take several minutes) before starting the next snapshot in the same manner.

7. Close the SQL Server Management Studio

Reporting Services Servers
This tab is used to configure the location of Reporting Services (which is a pre-requisite for the Reporting Extensions component).

1. Click **New**
2. Enter the following details:
3. **Hostname** From the drop-down list, select a server on which Reporting Services has been installed
5. **Primary** Check this when entering the Side A server. If the Side A server has already been configured, this checkbox will be disabled
6. Click **Test** to check the connection
7. Click **OK**
8. Repeat until all servers hosting Reporting Services have been entered

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

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

**NAMs**

**Note** This tab is relevant to IPCC Hosted Edition only.

This is used to configure servers hosting NAMs: ICMs that control other CICMs.

1. Click the **NAM** tab. A table is displayed, with seven columns, that will show information about the NAMs once they have been configured
2. To create a new NAM instance, click the **New** button. The **NAM Configuration** dialog window is displayed
   - **Instance Name** Enter a unique name to represent the NAM instance
   - **Server** Select the server that is hosting the NAM from the drop down list of the servers you configured on the **Servers** tab earlier
   - **Database Connection Parameters** Select the radio button of the login credentials you wish to apply:
     - **Windows authentication** This is the recommended option
- **SQL Server authentication** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your **Login Name** and **Password** in the fields provided.

- **ICM Instance** Select the correct ICM to use from a drop-down list of those available on the selected server.

- **HDS** In some deployments, real time and historical data may be held separately. Check this box if the specified NAM holds only historical data.

- **AWDB Catalog** The name of the administrative workstation database catalog, such as nam_awdb. This is configured automatically.

- **HDS Catalog** The name of the historical data server catalog, such as nam_hds. This is configured automatically.

- **Common ConAPI Credentials** Set up the credentials required to connect to the CICM/ICM.

  - **Application Name** Enter the name of the application you created on the CICM/ICM earlier.

  - **Application Key** Enter the password of the application you created on the CICM/ICM earlier.

  - **Remote Registry Port** The port to connect to on the CICM/ICM. This should be 2099.

  - **Local Registry Port** This should be the same as that set up in the CMS Control Console earlier, and must be unique for each CICM.

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

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

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

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

  - **Domain Controller A** Enter the name of the Domain Controller.

  - **Domain Controller B** Enter the name of the Side B Domain Controller if present.

  - **Use Secure Authentication** Select this checkbox in order to login to the domain controller as a specified user.

  - **Username** Enter the name of the domain user, such as NAMSERV\administrator.
• **Password** Enter the domain user’s password

4. Click **Refresh**

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

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

**CICMs**

This is used to configure the ICMs used by IPCC Enterprise Edition, or the CICMs used by IPCC Hosted Edition. Throughout this tab, ‘CICM’ refers to both CICM and ICM.

1. Click the **CICM** tab. A table is displayed, with seven columns, that will show information about the CICMs once they have been configured

2. To create a new CICM or ICM instance, click the **New** button. The **CICM Database Configuration** dialog window is displayed

   • **Instance Name** Enter a unique name to represent the CICM/ICM in VIM
   
   • **Server** Select the server that is hosting the ICM from the drop down list of the servers you configured on the **Servers** tab earlier
   
   • **Database Connection Parameters** Select the radio button of the login credentials you wish to apply:
     
     • **Windows authentication** This is the recommended option
     
     • **SQL Server authentication** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your **Login Name** and **Password** in the fields provided
   
   • **ICM Instance** Select the correct ICM to use from a drop-down list of those available on the selected server
   
   • **HDS** In some deployments, real time and historical data may be held separately. Check this box if the specified ICM holds only historical data
   
   • **AWDB Catalog** The name of the administrative workstation database catalog, such as cicm_awdb. This is configured automatically
   
   • **HDS Catalog** The name of the historical data server catalog, such as cicm_hds. This is configured automatically
   
   • **Common ConAPI Credentials** Set up the credentials required to connect to the CICM/ICM. These fields will be greyed out until the Provisionable checkbox has been checked
     
     • **Application Name** Enter the name of the application you created on the CICM/ICM earlier
     
     • **Application Key** Enter the password of the application you created on the CICM/ICM earlier
- **Remote Registry Port** The port to connect to on the CICM/ICM. This is usually 2099
- **Local Registry Port** This should be the same as that set up in the CMS Control Console earlier, and must be unique for each CICM
- **Provisionable** This indicates that the CICM is to be provisioned by the Portal, and should be checked
- **NAM Based** Check this box
- **Dual Sided** Check this box if you are using a dual-sided ICM. You will then be able to fill in details for Side B
- **Multi Media Support** Check this box if you are using a Cisco Unified Web and E-Mail Interaction Manager application instance in order to provide support for non-voice interactions

3. Click the **Configure Active Directory Mapping** button. The **Browse Active Directory** dialog window is displayed. This is used to provision the domain users who are required for supervisor memberships. The domain user must be a member of the domain active directory
   - **Domain Controller A** Enter the name of the Domain Controller
   - **Domain Controller B** Enter the name of the Side B Domain Controller if present
   - **Use Secure Authentication** Select this checkbox in order to login to the domain controller as a specified user
   - **Username** Enter the name of the domain user, such as CICMSERV\administrator
   - **Password** Enter the domain user’s password

4. Click **Refresh**

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

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

**CallManagers**

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

2. To add a CallManager click **New**

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

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

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

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

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

- **Server** Select the server hosting the CallManager that you configured on the Servers tab earlier.

- **Version** Select the required CallManager version.

- **Endpoint** Enter the URL used to access the CallManager AXL interface. The default is the default URL for the CallManager version selected.

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

- **Password** Enter the CallManager Administrator user’s password.

- **Test** Click to test the connection to the configured CallManager.

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

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

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

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

7. Click **OK**

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

4. **Connection Manager**

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

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

**Note** In some cases, such as where the source and/or target are dual sided, more than one connection may be created.
The connection types are:
- IN Datasource
- CICM/NAM AWDB
- CICM/NAM HDS
- CallManager

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

5. **Global Properties**

This configures advanced properties. For most installations there is no need to edit these.
- Java RMI Server Host Name This may need to be configured in cases where the Database Server has two network cards. Enter the IP address to be used by the ConAPI connection from the ICM
- Additional VM Parameters Indicates any additional parameters for use when connecting to the Java Virtual Machine

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

**Save / Revert**

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

**View Configuration Summary**

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

**Import/Export Configuration**

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

To export the configuration:

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

To import a previously-saved configuration:

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

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

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

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

Preparing the Configuration

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

- Make a note of the Host Name and IP Addresses of ALL of the machines that are hosting CVP
- Make a note of the User Name and Password of an administrative user on the domain so that you can configure File Replication and the Distributed File System
- Ensure that the Distributed File System, File Replication and Remote Procedure Call services are running on all of the CVP Servers and the Domain Controller

Configuring DFS for CVP Media File Upload

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

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

Note This folder requires full access security permissions for the Domain Computers group. Configure this for both the shared permissions and the security credentials.
8. Click Finish to complete the action and add the root to the DFS utility

**Configuring DFS Root Targets**
For each media server that the CVP Media File Upload should add files to, perform the following actions:
1. Right click on the new root and select the New Root Target option from the menu
2. Enter the Server Name for the CVP Server
3. For the Folder to Share, select the folder to contain the CVP media files that are uploaded

Note This folder requires full access security permissions for the Domain Computers group. Configure this for both the shared permissions and the security credentials.
4. Click Next to create the Root Target

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

**Configuring File Replication for CVP Media File Upload**
DFS shares must be setup on all the machines to which the media files should be copied, and file replication enabled among all of them.

The following steps will take you through the process of replicating files between the DFS shares. To enable this functionality you will need to ensure that the File Replication service is set to Automatic and is currently running. To begin file replication perform the following steps:
1. Logon to the Domain Controller as an administrative user
2. Click Start > Program Files > Administrative Tools > Distributed File System to open the Distributed File System configuration utility
3. Right click on the Distributed File System node in the left hand panel and select the Show Root option
4. Select the PortalMedia node
5. Right click on the PortalMedia node located in the left hand panel of the Distributed File System window. Select the Configure Replication option from the menu. The Configure Replication Wizard is displayed.
6. When prompted to select the initial master select the share located on the domain controller
7. Select the **Full Mesh** topology for the replication set
8. Click the **Finish** button to set up replication between the selected folders

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

## Performance Configuration Checklists

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

### Web Server

<table>
<thead>
<tr>
<th>Done</th>
<th>Description</th>
</tr>
</thead>
</table>
| ✗    | Add the `/3GB boot.ini` switch to all systems with more than 2GB memory.  
  - Right-click **My Computer** and select **Properties**. The **System Properties** dialog box is displayed.  
  - Click the **Advanced** tab.  
  - In the **Startup and Recovery** area, click **Settings**. The **Startup and Recovery** dialog box is displayed.  
  - In the **System startup** area, click **Edit**. This opens the Windows `boot.ini` file in Notepad.  
  - In the line that states “`WINDOWS="Microsoft"`, add the following to the end of the line: `/fastdetect switch: /3GB`.  
  - Save the changes and close Notepad.  
  - Click **OK** twice to close the open dialog boxes. Reboot for the changes to take effect. |
| ✗    | For the IIS DefaultAppPool: disable **IIS6 App Pool Shutdown** |
| ✗    | Edit `RSReportServer.config`: set `MaxActiveReqForOneUser = 100`  
  `RSReportServer.config` can be found in `C:\Program Files \Microsoft SQL Server \MSSQL \ReportServer` |
| ✗    | Edit `RSReportServer.config`: set `CleanupCycleMinutes = 1200` |
| ✗    | Edit `RSReportServer.config`: add a key |
WebServiceUseFileShareStorage = true in the same section as the previous two updates:

<Add Key="WebServiceUseFileShareStorage" Value="true" />


## Database Server

<table>
<thead>
<tr>
<th>Done</th>
<th>Description</th>
</tr>
</thead>
</table>
| ☐    | Add the `/3GB boot.ini` switch to all systems with more than 2GB memory.  
1. Right-click My Computer and select Properties. The System Properties dialog box is displayed.  
2. Click the Advanced tab.  
3. In the Startup and Recovery panel, click Settings. The Startup and Recovery dialog box is displayed.  
4. In the System startup panel, click Edit. This opens the Windows boot.ini file in Notepad.  
5. In the line that states “WINDOWS="Microsoft”, add the following to the end of the line: `/fastdetect switch: `/3GB  
6. Save the changes and close Notepad.  
7. Click OK twice to close the open dialog boxes. Restart the computer for the change to take effect. |
| ☐    | Defragment page file and registry hives using http://www.sysinternals.com/Utilities/PageDefrag.html |
| ☐    | Split ReportServerTempDB into multiple files |
5. POST INSTALLATION STEPS

Logging into the Management Portal

The Management Portal can now be opened from Start > All Programs > Management Portal > Web > Management Portal. This will open a web page, which you can bookmark.

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

For login to a new system, use the username ‘administrator’ and a blank password. You will be prompted to change this. If you are logging into an upgraded system, the administrator password will not have changed from that previously used.

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

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

Report Uploading

The audit report template must be uploaded into the system. To upload the report into the Unified Contact Center Management Portal system:

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

The Upload Audit Reports dialog window is displayed.

1. Enter administrator in the User Name field
2. Enter your administrator password in the Password field

Note You must have specified a new administrator password in the Management Portal, as described above, in order to perform this task

3. Click Upload

The Report Uploader now transfers the report template from the folder in which it was installed to a shared folder for users to access.
6. UPGRAADING FROM A PREVIOUS VERSION

This chapter details how to upgrade from previous Management Portal versions to version 7.5(1).

Overview

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

Caution You should back up all your servers, especially your publisher database server, before you begin.

Uninstalling the Portal

Uninstalling Data Import Server Component

This process will remove the Data Import Server component. This will remove the ability to import data from remote datasources (such as ICM or CallManager) to the Unified Contact Center Management Portal datamart.

Removing Replication

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

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

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

You may now remove replication.

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

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

Once replication has been successfully removed then you may proceed.

**Uninstalling Data Import Server Component**

1. In your Windows desktop, click **Start > Control Panel > Add or Remove Programs**. The **Add/Remove Programs** list is displayed.
2. Select **Management Portal: Data Import Server**
3. Click the **Remove** option. A dialog window is displayed asking you if you are sure that you wish to remove the **Management Portal: Data Import Server**
4. Click **Yes**. The **Setup Status** dialog window is displayed. The extent of the uninstallation progress is displayed on the progress bar
5. Restart if prompted to do so

**Uninstalling the Provisioning Server Component**

This process will remove the Provisioning Server component, removing the Unified Contact Center Management Portal connection for any remote datasources, such as CICM/ICM or CallManager.

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

1. Select **Management Portal: Provisioning Server**
2. Click the **Remove** option and confirm
3. When prompted, click **Yes** to complete uninstallation and restart the system
4. Manually delete the folder: `C:\Program Files\Management Portal\Provisioning Server\Config`

**Uninstalling Other Components**

All the other components of the Management Portal may be uninstalled by simply clicking **Remove** from the **Add/Remove Programs** window. These should be uninstalled in the following order:

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

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

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

Once uninstallation is complete the ReportServer service should be restarted.

Upgrading SQL Server

Upgrading to SQL Server 2005 Enterprise Edition

Upgrading SQL Server

Insert your SQL Server 2005 Enterprise Edition CD and begin the upgrade process, clicking Next to go through the screens in turn.

When prompted to select components, check the boxes for the following:

- SQL Server Database Services
- Reporting Services
- Workstation Components

Configuring the NT AUTHORITY\NETWORK SERVICE account

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

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

Upgrading to SQL Server 2005 Standard Edition

Backing Up Databases
You will need to back up the Portal and ReportServer databases in order to restore them after installing SQL Server 2005.

1. Go to Start > All Programs > Microsoft SQL Server > Enterprise Manager
2. Navigate to the Portal database
3. Right-click on Portal and select Backup. Save the .bak file to a suitable location
In most cases the .bak file is sufficient to restore the database, but if this fails you will need to restore from the data files. Back these up as described below:
1. Right-click on Portal and select Detach database. This will ensure that the data files are in a stable state for copying
2. Manually copy the data files to a suitable location
In a similar fashion, back up the ReportServer databases:
1. Run the command services.msc
2. Stop the ReportServer service
3. Using the Enterprise Manager, backup the ReportServer and ReportServerTempdb databases
4. Detach the ReportServer and ReportServerTempdb databases
5. Save the data files to a suitable location
6. In the Enterprise Manager, attach the ReportServer and ReportServerTempdb databases again
Note The process for upgrading SQL Server 2000 Enterprise Edition to SQL Server 2005 Standard Edition assumes that the ReportServer databases are connected. If you do not reattach the databases after copying the files the upgrade will fail.
7. Run services.msc and restart the ReportServer service

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

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

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

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

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

4. Run the `services.msc` command and stop the SQL Server Reporting Services (`{MSSQLSERVER}`) service
5. Go to Start > All Programs > Microsoft SQL Server > Management Studio
6. Click the Restore Database option
7. Select the backup files to restore the ReportServer and ReportServerTempDB databases
8. Note The default path for ReportServer data files differs between SQL Server 2000 and SQL 2005. To see or change the location to which the databases will be installed, go to the Options page

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

Restoring the Databases from the Data Files

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

For the Portal database:

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

For the ReportServer and ReportServerTempDB database:

1. Ensure the SQL Server Reporting Services (`{MSSQLSERVER}`) service is stopped
2. Detach the ReportServer and ReportServerTempDB databases
3. Copy the SQL Server 2005 ReportServer and ReportServerTempDB data files to a suitable location in case the changes need to be reverted
4. Delete the original SQL Server 2005 ReportServer and ReportServerTempDB data files
5. Replace the SQL Server 2005 ReportServer and ReportServerTempDB data files with the SQL Server 2000 data files
ReportServer and ReportServerTempDB data files that you backed up earlier

6. Using Management Studio, click the Attach Database option and attach your backed up ReportServer and ReportServerTempDB databases

Note The default path for ReportServer data files differs between SQL Server 2000 and SQL 2005

7. Run services.msc and restart the ReportServer service

You can now upgrade the databases.

Upgrading the Databases

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

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

It will also be necessary to delete the old encryption keys and set up new ones.

1. From the Reporting Services Configuration Manager select Encryption Keys
2. Click Delete and confirm
3. Click on Initialization
4. Check the box for the first key and click Remove
5. Click Initialize and a new key will be created
6. Restart the computer

Configuring the NT AUTHORITY\NETWORK SERVICE account

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

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

Installing the Portal

Install the new version of the Management Portal as described in Chapter 3 Component Installation. During installation of the Database Component, you must select the option to upgrade an existing database rather than installing a new database.

Configuration

Configuration Manager

1. Open the Portal’s Configuration Manager from Start > All Programs > Management Portal > Configuration Manager
2. Click on UCCMP Servers
3. On the Application Servers tab:
   • From the left-hand list of servers in the cluster, check the server which is to be the Side A Web Server
   • Use the arrow button to move it to the Primary Application Servers list
   • If there is a Side B Web Application Server, check the Dual Sided checkbox
   • Select the server which is to be the Side B Web Server and move it to the Secondary Application Servers list
4. On the Reporting Services Servers tab:
   • Click New
   • Enter the following details:
     • Hostname From the drop-down list, select a server on which Reporting Services has been installed
     • ReportServer Url Enter the web address of the Reporting Services server. For example, http://SIDEA/ReportServer/ReportService.asmx
     • Primary Check this when entering the Side A server. If the Side A server has already been configured, this checkbox will be disabled
     • Click Test to check the connection
     • Click OK
     • Repeat until all servers hosting Reporting Services have been entered
5. On the **Reporting Services Databases** tab:
   - Select the existing ReportServer database
   - Click **Edit**
   - Click **Test** to check the connection

6. On the **Portal Databases** tab:
   - Test the connections as above

7. Close the **UCCMP Servers** window

8. Click on **Communication Servers**

9. Select the **CICMs** tab

10. Edit each CICM in turn and check its details

11. Ensure the **Provisionable** checkbox is checked for each CICM

12. Restart the computer

### Setting up ReportServer Connections

1. In Internet Explorer, open up the URL `<SERVERNAME>/Reports`

2. Click on **AWDB**

3. Fill in the connection strings to be used by ReportServer to connect to the AWDB

4. Repeat for **Portal**

### Replication

To set up replication on the upgraded system:

1. Open the Portal Databases tab on the **Configuration Manager**

2. Click **Replication** to open the **Cisco Database Replication Configuration** dialog window

3. Click the **Replicate** button and confirm

4. Click **OK** to close the Cisco Database Replication Configuration window

5. Click **Apply**, then **Close**

6. Now log onto the Subscriber and open the **SQL Server Enterprise Manager**, then open the **Replication Monitor**. Under **Agents/Snapshot Agents** three snapshot agents are listed

7. Start the first snapshot agent (that for the **Base** publication) by right clicking on the agent and selecting **Start Agent**. Wait for the snapshot status to change to ‘succeeded’ (this may take several minutes) before starting the next snapshot in the same manner.

8. Close the SQL Server Enterprise Manager

Your upgraded version of the Management Portal should now be fully operational.
7. PLATFORM UNINSTALLATION

This chapter details how to remove the Unified Contact Center Management Portal platform components from the platform. The uninstallation procedure should be performed in the following order:

**Uninstalling Data Import Server Component**

This process will remove the Data Import Server component. This will remove the ability to import data from remote datasources (such as ICM or CallManager) to the Unified Contact Center Management Portal datamart.

**Removing Replication**

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

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

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

*Note* Removing replication may take some time.

Once replication has been successfully removed then you may proceed.

**Uninstalling Data Import Server Component**

1. Insert the CD that came with your old version of the Management Portal. Close any windows that automatically open
2. In your Windows desktop, click Start > Control Panel > Add or Remove Programs. The Add/Remove Programs list is displayed.
3. Select **Management Portal: Data Import Server**

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

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

**Uninstalling the Database Component**

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

**Caution** If upgrading an existing version of the Management Portal, **DO NOT** perform this step as it will remove all your existing data

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

**Uninstalling All Other Components**

All the other components of the Management Portal may be uninstalled by simply clicking **Remove** from the **Add/Remove Programs** window. These should be uninstalled in the following order:


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

A

Audit
A diagnostic process instigated to assess system performance.

C

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

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

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

Cipher
A method used to encrypt text.

Cluster
Multiple networked servers, which form the platform across which the Unified Contact Center Management Portal is deployed.
Commissioning
Any action or process required to setup the Unified Contact Center Management Portal platform that is not setup by the Unified Contact Center Management Portal installer or inherent tools.

Configuration
The hardware and/or software components, which comprise a system and the manner in which they are connected.

Connection
The link between two nodes in a script or between a node and a routing target set. Connections show the flow of control between objects in the script. Within the Script Editor, a connection is represented as a line segment.

Connectors
Connectors consist of:
- Telephony connectors which the Unified Contact Center Management Portal uses to interface with routing components during call routing.
- Business connectors which the Unified Contact Center Management Portal uses to interface with back office databases to collect data used to determine the route of the call or to be packaged with the call to inform the contact center agent.

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

Comma Separated File (.CSV)
A method of representing a spreadsheet using a text file. The values are separated by commas, and each record is ended by a line break. The column headers are contained in the first record.
Domain
On the Internet, domains are defined by the IP address. All the networked computers and devices sharing a common part of the IP address belong to the same domain. They are administered as a whole unit with the same rules and procedures.

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

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

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

Field
A space in a database allocated to an item of information. A collection of fields is called a record.

Firewall
A security measure placed between trusted and un-trusted sites. It filters out traffic, which can damage the host network or connected hardware.

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

Graphical User Interface (GUI)
A point and click interface within Windows applications allowing the user to interact with a software program without the need to write code.
Hash
The Unified Contact Center Management Portal uses hashed values for security purposes. A hash value or message digest is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is highly likely to be a unique value. They are used to ensure that transmitted messages have not been tampered with. The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they are identical, there is a high probability that the message was transmitted intact.

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

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

Logger
A software application that logs events.

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

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

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

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

Secure Sockets Layer (SSL) – (See HTTPS)

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

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

SQL Server
The Microsoft relational database product used for the ICM’s local and central databases.
String
A series of characters, which have been arranged into a specific grouping in a coded script.

Synchronous
Occurring at regular intervals. The opposite of synchronous is asynchronous. Communication within a computer is usually synchronous and is governed by the microprocessor clock, for example, signals along the bus can occur only at specific points in the clock cycle.

Thread
A part of a program that can be executed independently of other parts.

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

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

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

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

<table>
<thead>
<tr>
<th>A</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Instance List...26</td>
<td>ICM..........................9</td>
</tr>
<tr>
<td>Audit........8</td>
<td>IPCC..........................9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B</th>
<th>L</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back up.........14</td>
<td>Load balancing........10</td>
</tr>
<tr>
<td>BITS ........12</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>CallManager ..........9</td>
<td>Microsoft Distributed File System36</td>
</tr>
<tr>
<td>CICM................9, 25, 32</td>
<td>Microsoft Terminal Services ......12</td>
</tr>
<tr>
<td>Cisco Security Agent (CSA)......16</td>
<td></td>
</tr>
<tr>
<td>Cluster .............24</td>
<td></td>
</tr>
<tr>
<td>CMS Server ..........26</td>
<td></td>
</tr>
<tr>
<td>Commission ..........8</td>
<td></td>
</tr>
<tr>
<td>Component ...........11</td>
<td></td>
</tr>
<tr>
<td>ConAPI...............25</td>
<td></td>
</tr>
<tr>
<td>Connections ..........34, 49</td>
<td></td>
</tr>
<tr>
<td>CVP Media File Upload.....36</td>
<td></td>
</tr>
<tr>
<td>CVP tools ..........9</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data replication ..........24</td>
<td>NAM........................25</td>
</tr>
<tr>
<td>Database</td>
<td>NT AUTHORITY\NETWORK SERVICE ........15, 44, 47</td>
</tr>
<tr>
<td>Back up..................45</td>
<td></td>
</tr>
<tr>
<td>Replication.............20, 24, 49</td>
<td></td>
</tr>
<tr>
<td>Restore................20, 46</td>
<td></td>
</tr>
<tr>
<td>Decrypt................18</td>
<td></td>
</tr>
<tr>
<td>Dedicated Server ..........10</td>
<td></td>
</tr>
<tr>
<td>Demilitarized zone (DMZ)....10</td>
<td></td>
</tr>
<tr>
<td>Deployment</td>
<td></td>
</tr>
<tr>
<td>Models..................10</td>
<td></td>
</tr>
<tr>
<td>Specifications ........9</td>
<td></td>
</tr>
<tr>
<td>Distributor ........9, 24</td>
<td></td>
</tr>
<tr>
<td>Documentation ..........23</td>
<td></td>
</tr>
<tr>
<td>Domain controller ..........12</td>
<td></td>
</tr>
<tr>
<td>Dual-sided ...........16</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt .......18</td>
<td>Performance Configuration</td>
</tr>
<tr>
<td>Encryption keys ..........47</td>
<td>Checklists ........38</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>F</th>
<th>R</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP...............12</td>
<td>Reboot ........12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>G</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Secure Deployment....10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>H</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Transaction log.....14</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>