Installation Guide for Cisco Unified Contact Center Management Portal

Release 7.1(1)

August 2006

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 (64387)
Fax: 408 526-4100

CONTENTS

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”

Describes the integration between the Unified Contact Center Management Portal and IPCC Hosted Edition and how the Unified Contact Center Management Portal adds value to the system. It describes how the Unified Contact Center Management Portal is used to configure (commission) a system deployment and manage that system.

Chapter 2, “Installation Guidelines”

Describes the general prequisites for the Unified Contact Center Management Portal installation, including platform and back up servers, antivirus software, security accounts, monitoring, system management and data replication between servers.

Chapter 3, “Component Installation”

Provides installation and configuration checklists for the Database, Application, Reporting Services, Web, Provisioning and Data Import server components.

Chapter 4, “Database Component”

Describes the procedure to install the Unified Contact Center Management Portal Database component and also describes server security configuration.

Chapter 5, “Reporting Component”

Describes the procedure to install the SQL Server Reporting Services component and Service Pack, including the installation of the .NET Framework 2.0 Runtime and Reporting extensions.

Chapter 6, “Application Component”

Describes the procedure to install the Reporting Services Application extensions.

Chapter 7, “Web Component”

Describes the procedures to install the Web component and Office Web Components, Web component server configuration and

security configuration, user account creation and the event viewer setup.

Chapter 8, “Provisioning Component”

Describes the procedure to install the Unified Contact Center Management Portal Provisioning component.

Chapter 9, “Data Import Component”

Describes the procedure to install the Unified Contact Center Management Portal Data Import component.

Chapter 10, “Product Documentation”

Describes the procedure to install the accompanying user manuals from the Unified Contact Center Management Portal CD.

Chapter 11, “Component Configuration ”

Describes configuration details for the Unified Contact Center Management Portal platform components, including the setting of Database server user accounts and roles, Provisioning component server connector configuration, IIS 6.0 enabling on the Web component servers, Data Import component data source connectivity, password encryption and uploading .wav files for voice announcements. The procedure to configure 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 12, “Post Installation Steps”

Describes how to upload report templates into the Unified Contact Center Management Portal platform.

Chapter 13, “Component Uninstallation”

Describes the procedure to uninstall the Unified Contact Center Management Portal platform components.

Chapter 14, “Glossary”

Describes the terms used in relation to the Unified Contact Center Management Portal environment.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems

Attn: Customer Document Ordering

170 West Tasman Drive

San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies — security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered non-emergencies.

- Non-emergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting show command output. Search results

show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- iQ Magazine is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with

Cisco experts and other networking professionals. Join a discussion at this URL:

http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

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 Hosted Edition. The Unified Contact Center Management Portal serves two mutually supportive purposes:

- **Simplify** the operations and procedures for performing basic tasks such as Move/Add/Modify Agents, Skill Groups, Teams and other common administrative functions.
- **Provide a common web user interface** within the product set. Currently, IPCC Hosted Edition and CallManager use different interfaces. Simple tasks therefore require performing multiple tasks in both products to achieve a single goal, for example, adding an agent. By providing a web-based unified interface for common administrative tasks, the value of the solution increases, by decreasing the amount of time, knowledge, training and resources currently required to administer the solution set.

The Unified Contact Center Management Portal components comprise a module that is integrated with IPCC Hosted Edition. IPCC Hosted Edition customers can optionally include the Unified Contact Center Management Portal to satisfy particular business requirements.

Primary Functionality

- **Unified Configuration**, that is, tenant provisioning of both the applicable IPCC Hosted Edition CICM and CallManager components through a single task-based web interface.
- **Hierarchical Administration**, for example:
  - The Service Provider Administrator can add a Tenant.
  - The Tenant Administrator can add a Skill Group.
  - The Tenant Supervisor can add an Agent.
- **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. Examples include installing PGs and configuring PGs and Network Trunk Groups.

- **Provisioning** consists of day to day configuration operations performed by a tenant. Examples include Move/Add/Modify Agents, Skill Groups and Teams.

The Service Providers will use the existing IPCC Hosted Edition, CallManager and CVP tools (installers and configuration tools) to commission a system. Service Providers will use the Unified Contact Center Management Portal Provisioning System to define tenants and set up tenant permissions. Tenants will then use the Unified Contact Center Management Portal Provisioning System to provision their specific site.

The Unified Contact Center Management Portal provides a provisioning layer on top of IPCC Hosted Edition 7.1. It works with the standard IPCC Hosted Edition, a new single-instance IPCC Hosted Edition Deployment and CallManager.

The Unified Contact Center Management Portal provides its own provisioning database that includes a rich, hierarchical permissions model. Provisioning changes are stored in the Unified Contact Center Management Portal system and then exported to IPCC Hosted Edition and CallManager.

Additionally, the Unified Contact Center Management Portal system can read existing configuration data from IPCC Hosted Edition and CallManager, store them in the Unified Contact Center Management Portal database and reconcile differences between them. This enables Service Providers to make configuration changes using existing IPCC Hosted Edition and CallManager tools and propagate these changes into the Unified Contact Center Management Portal system.

Deployment Specifics

Unified Contact Center Management Portal platform deployments are limited to standard IPCC Hosted Edition deployments with the following restrictions:

- Each Tenant must have its own:
  - CICM instance.
  - Dedicated Admin Workstation Real Time Distributor server.

Note: Multiple Distributor instances on a single server are NOT allowed.

  - WebView instance for reporting purposes.
- The Unified Contact Center Management Portal is only supported on IPCC Hosted Edition 7.1 and above.
- Current IPCC Enterprise Edition customers can deploy the Unified Contact Center Management Portal in their system to provide particular features – thereby converting that system to a NAM-less IPCC Hosted Edition model. (However, multi-level access/ partitioning is not currently provided for reporting or agent statistics).

Deployment Models

N-Sided Replication

In most deployments, the Unified Contact Center Management Portal is installed on a dual sided basis to provide load balancing, resilience and high availability. For deployments that require layered security, for example, 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 consultation with a certified systems integrator 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.

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

2. INSTALLATION GUIDELINES AND REQUIREMENTS.

General Advice

- Reboot the server after the installation has finished, making sure that the Unified Contact Center Management Portal Provisioning component service starts automatically on boot.
- Do NOT install the Unified Contact Center Management Portal platform on a domain controller.
- Do not enable IIS logging. The Unified Contact Center Management Portal Provisioning component provides a real time monitoring web site that automatically updates every five seconds. Therefore if logging is enabled, very large log files can build up on the server.
- The SQL Server Agent service is required to summarize Unified Contact Center Management Portal Provisioning component audit information. It runs a SQL Server job periodically to compress the real time request table into a summarized request half hour table.
- Configure the Unified Contact Center Management Portal to produce SNMP traps. (Please see the accompanying manual; Administration Guide for Unified Contact Center Management Portal Release 7.1).
- Configure the Unified Contact Center Management Portal Provisioning component service to restart automatically if it fails (this is configured using the Windows Service Control panel applet).
- Install all the Unified Contact Center Management Portal Provisioning component pre-requisites and connectors on the Provisioning component server and configure as dual mode (not clustered).
- Norton Antivirus may state that the **autorun.hta** script file is malicious. Please ignore and continue with the installation as per normal.

Server Guidelines

- Install Windows 2003 Service Pack 1 on all the servers hosting the Unified Contact Center Management Portal.
- 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*.

- On the Database Servers install SQL Server 2000 Enterprise Edition.
    - When installing the SQL Server 2000 database application, accept the default settings.
    - Install SQL Server using *mixed-mode authentication* and use *local system* for the SQL Server and SQL Agent startup accounts.
- Install all the latest Service Packs for: Windows 2003 (Service Pack 1), SQL Server 2000 Enterprise Edition (Service Pack 4) and Microsoft .NET v.1.1 (Service Pack 1).
- Harden the Internet Information Services Web Server (IIS) and SQL Server 2000 according to Microsoft's latest guidelines.
- Disable all unnecessary local services (FTP, BITS and so forth).
- Use Microsoft Terminal Services for remote configuration and support.

Server Backups

- Regularly back up the SQL Server databases and truncate transaction logs to prevent them becoming excessively large.
- Schedule back-ups 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.
- The built-in NETWORK SERVICE account is used extensively. A set of steps to configure various areas of the application to run as a network service are carried out during and after installation. These steps are detailed later in this document. When installing components that require a SQL Server Database connection you will be asked whether or not you would like to use Windows Authentication or SQL Server Authentication. Data access will be achieved using the build-in NETWORK SERVICE account if Windows Authentication is selected.

Windows Components

The following windows components are required for installation:

- **Microsoft Message Queuing**. (See page 33).
- **Microsoft Windows 2003 Application Server with ASP.NET components (IIS)**. (See pages 32 and 39).
- **Microsoft .NET Framework 1.1**. (This is enabled as part of the Application server role configuration performed during the Windows 2003 installation).
- **Microsoft Reporting Extensions** (which are enabled by default during the Microsoft Reporting Services installation).
- **Microsoft Internet Explorer 6.0**. (Installed by default as part of Windows 2003).
- **Microsoft Script Host** (Installed by default as part of Windows 2003).
- **Network Com+ Access**. (This is enabled as part of the Application server role configuration performed during the Windows 2003 installation).

Installation Prerequisite Checklist

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

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

Each individual component installation guide includes these prerequisites, however here is a summary.

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.
- Microsoft SQL Server 2000.
- Microsoft SQL Server 2000 SP4.

Reporting Services

- Windows Installer 3.1
- Microsoft .NET Framework 1.1
- Microsoft WSE 2.0 SP3
- Microsoft SQL Server 2000 Reporting Services SP2

Application

- Windows Installer 3.1

- Microsoft .NET Framework 2.0
- Microsoft WSE 2.0 SP3
- Reporting Extensions

Web

- Windows Installer 3.1
- Microsoft .NET Framework 2.0
- ASP .NET State Service 2.0

Provisioning

- Windows Installer 3.1
- J2SE Runtime Environment 5.0
- MSXML 4.0 SP2 Parser

Data Import

- Windows Installer 3.1
- Microsoft .NET Framework 2.0

3. COMPONENT INSTALLATION

To install the Unified Contact Center Management Portal platform requires an understanding of the components, the environment in which they are deployed and how they are configured in a cluster of linked servers. File systems and storage options are discussed as well as user account and security considerations in an internet facing environment. This chapter details how to prepare your servers for installation, including operating systems, service packs and prerequisites.

Planning Your Installation

The Unified Contact Center Management Portal consists of the following components:

- Database
- Reporting Extensions
- Application
- Web
- Provisioning
- Data Import

These components can be installed on one or more computers and in a wide range of different configurations. This flexibility allows for customizable levels of performance, scalability and resilience.

- The **Database** component utilizes an application called the **Importer** to import enterprise data from one or many different data sources into a Microsoft SQL Server 2000 based Management Information Database.
- The **Application** component manages security by ensuring that users can only view specific content defined by their security login credentials. The Application component also manages failover so if the connection to one database server fails, the application can automatically retrieve the required data via an alternative database connection.
- The **Web** component provides the interface that allows users to interact with data from the various sources of the application. They may perform reporting, administrative or provisioning tasks with this data.
- The **Provisioning** component and its library of connectors enable it to communicate with network equipment assisting in making intelligent call routing decisions. It communicates with back office databases and other third party systems to extract information for routing and reporting purposes.

- The **Data Import** component is an Extract, Transform and Load (ETL) server for data warehouses. The Data Import component imports the data used to build reports. It is designed to handle high volume data (*facts*) such as call detail records as well as data that is changed irregularly (*dimensions*) such as agents, peripherals and skill groups. It is highly configurable by design so that it can be applied to a wide range of data processing problems; however, its principle design goal is as an ETL runtime application.

The installation interface will guide you through the installation process. Make sure that you have the relevant CDs and are connected to the internet to download any of the required prerequisites if necessary.

Once the platform components and prerequisite applications have been installed, configuration is required. Please see chapter 11.

Note: For dual-sided, or replicated systems, it is recommended that a complete installation is 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 11, can be performed.

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

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

4. DATABASE COMPONENT

This chapter details how to install and configure the Unified Contact Center Management Portal Database server components, including SQL Server 2000 Enterprise Edition and the Unified Contact Center Management Portal Database component.

Please note that if the Unified Contact Center Management Portal server cluster comprises more than one database component server, the procedure below has to be repeated on all servers hosting database components.

Database Component Installation

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

1. If autorun is disabled and you have not been presented with the Unified Contact Center Management Portal Products Installation Application then double click the **autorun.bat** to launch the Unified Contact Center Management Portal installer.
2. Click the **Database Server** tab.

   The main panel is refreshed. A list of software applications that need to be installed before the Database component can be installed are displayed beneath the **Prerequisites** header. The following prerequisite applications are listed.

   - Windows Installer 3.1.
   - Microsoft SQL Server 2000.
   - Microsoft SQL Server 2000 SP4.
3. Click the **Run Test…** button.

The system checks if the above prerequisite applications are installed.

Any prerequisite application that is installed is displayed with a green tick next to it. Conversely, any prerequisite application that is not installed is displayed with a red cross next to it.

Note: Any prerequisite that is not installed is required to be installed before the installation of the Database Component can proceed.

Once all the prerequisite software is installed click the **Re-Run Test…** button to enable the **Install** button.

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

The **Welcome to the Cisco Unified Communications** dialog window is displayed.

The **InstallShield** sets up the **InstallShield Wizard**.

The **Management Portal: Database Setup - InstallShield Wizard** is displayed.

1. Click **Next**.

The **License Agreement** dialog window is displayed.

1. Select the **I accept the terms in the License Agreement** checkbox.
2. Click **Next**.

The **Ready to Install the Program** dialog window is displayed.

1. Click **Install**.

The **Installing Management Portal: Database Setup** dialog window is displayed.

The **InstallShield Wizard Completed** dialog window is displayed. To install a database now:

1. Ensure that the **Launch Management Portal: Database Setup** checkbox is checked.
2. Click **Finish**.

If you wish to setup a database at a later time make sure the **Launch Database** checkbox is blank and click **Finish**.

To launch the database setup wizard manually, navigate to the installation folder (C:\Program Files\Management Portal\Database\Installer) and then run the **Portal.Database.Installer.exe** application.

The wizard will guide you through the process of creating the data mart.

The **Welcome to the Management Portal Database Installer Wizard** dialog window is displayed.

1. Click **Next**.

The **SQL Server Connection Details** dialog window is displayed.

1. In the **Server Name** field select the required 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 **(local)** should be selected.
2. In the **Database Name** field, enter or select the name of the database catalog that will be used for Unified Contact Center Management Portal.

Note: To simplify installation, name the SQL Server database **Portal**. This is the default setting.

3. In the **Connect Using** section select the radio button of the login credentials you wish to apply:
   - Windows login credentials.
   - SQL Server login credentials. If this option is selected enter your **Login Name** and **Password** in the fields provided.
4. Click the **Test Connection** button to make sure the connection to the SQL Server is established. If you are creating a new database and the connection is successful then you will be alerted that the *connection succeeded but the database does not exist*. Click **OK** to continue.
5. Click **Next**.

The **Select an Action to Perform** dialog window is displayed.

1. Select the **Install a new database** option.
2. Click **Next**.

The Configure the Location of Data Files dialog window is displayed.

1. Select the **File Groups** to be configured by selecting the checkboxes of the required File Groups, or
2. Click the **Select all** button to select all of the listed File Groups, or
3. Click the **Select None** button to leave the File Groups unselected.
4. Click the Up or Down buttons on the **Initial Size** and **Max Size** field to define the the storage capacity required for the selected files.
5. Click **Next**.

The **You have selected the following** dialog window is displayed.

1. To begin installation click **Next**.

The Setup **is performing your actions** dialog window is displayed.

The **Completing the Management Portal Database Installer Wizard** dialog window is displayed.

1. The database installation is now complete. Click **Close** to close the installation application..

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 11).

Database Component Configuration

Please see chapter 11.

5. REPORTING EXTENSIONS COMPONENT

This chapter details how to install and configure the Unified Contact Center Management Portal Reporting Extensions, including prerequisite software and SQL Server Reporting Services.

Reporting Extensions Component Installation

The Unified Contact Center Management Portal Reporting Extensions add further reporting functions. These functions include thresholds to apply to report data, advanced report parameters and enhanced security.

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

1. If autorun is disabled and you have not been presented with the Unified Contact Center Management Portal Products Installation Application then double click the **autorun.bat** to launch the Unified Contact Center Management Portal installer.
2. Click the **Reporting Extensions** tab.

   The main panel is refreshed. A list of software applications that need to be installed before the Reporting Extensions component can be installed are displayed beneath the **Prerequisites** header. The following prerequisite applications are listed.

   - Windows Installer 3.1
   - Microsoft .NET Framework 1.1
   - Microsoft WSE 2.0 SP3
   - Microsoft SQL Server 2000 Reporting Services SP2
3. Click the **Run Test…** button.

   The system checks if the above prerequisite applications are installed.

   Any prerequisite application that is installed is displayed with a green tick next to it. Conversely, any prerequisite application that is not installed is displayed with a red cross next to it.

   Once all the prerequisite software is installed click the **Re-Run Test…** button to enable the **Install** button.
4. If all the prerequisite applications have a green tick displayed next to them, click the **Install** button to install the Reporting Extensions component.

The **Welcome to the Cisco Unified Communications** dialog window is displayed.

The **Welcome to the Installshield Wizard for Management Portal: Reporting Extensions** dialog window is displayed.

1. Click **Next**.

The **License Agreement** dialog window is displayed.

1. Select the **I accept the terms in the License Agreement** checkbox.
2. Click **Next**.

The **Ready to Install the Program** dialog window is displayed.

1. Click I**nstall**.

The **Installing Management Portal: Reporting Extensions** dialog window is displayed.

The **InstallShield Wizard Completed** dialog window is displayed.

1. Click **Finish**.

6. APPLICATION SERVER COMPONENT

This chapter details how to install and configure the Unified Contact Center Management Portal Application Server components, including prerequisite software and the creation of user accounts.

Application Server Component Installation

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

1. If autorun is disabled and you have not been presented with the Unified Contact Center Management Portal Products Installation Application then double click the **autorun.bat** to launch the Unified Contact Center Management Portal installer.
2. Click the **Application Server** tab.

   The main panel is refreshed. A list of software applications that need to be installed before the Application component can be installed are displayed beneath the **Prerequisites** header. The following prerequisite applications are listed:

   - Windows Installer 3.1
   - Microsoft .NET Framework 2.0
   - Microsoft WSE 2.0 SP3
   - Reporting Extensions
3. Click the **Run Test…** button.

   The system checks if the above prerequisite applications are installed.

   Any prerequisite application that is installed is displayed with a green tick next to it. Conversely, any prerequisite application that is not installed is displayed with a red cross next to it.

   Once all the prerequisite software is installed click the **Re-Run Test…** button to enable the **Install** button.
4. If all the prerequisite applications have a green tick displayed next to them, click the **Install** button to install the Application Server component.

The **Welcome to the Cisco Unified Communications** dialog window is displayed.

The **Welcome to the Installshield Wizard for Management Portal: Reporting Application Server** dialog window is displayed.

1. Click **Next**.

The **License Agreement** dialog window is displayed.

1. Select the **I accept the terms in the License Agreement** checkbox.
2. Click **Next**.

The **Cryptography Configuration** dialog window is displayed.

1. Create a cryptographical pass phrase and enter it in the **Passphrase** field. It is recommended that the cryptography passphase be between 6 and 35 characters containing, lowercase, uppercase, numeric and alpha-numeric characters.

Note: This passphase is used for the encrypting and decrypting system passwords. You should make a record of the passphrase as it will be asked for during the installation of the Data Import component.

2. Re-enter the passphrase in the **Confirm Passphrase** field.
3. Click **Next**.

The **Application Server Location** dialog window is displayed.

1. If the Application is to be installed on a single sided platform (one server) select the **Standalone** radio button.
2. If a dual sided installation is being performed then select either **Side-A** or **Side-B** depending on the side which you are installing.
3. Click **Next**.

The Side-A Management Portal Database Connection dialog window is displayed.

1. In the **Side-A SQL Server** field enter the name of the server where the Unified Contact Center Management Portal database has been installed. For a dual-sided installation this will be the side-A database server.
2. In the **Side-A Catalog Name** field enter the name of the database. This is the name of the database created in the Database Component step performed earlier. By default this is **Portal.**
3. In the **Connect Using** section, select the radio button of either:
   - Windows authentication, or
   - SQL Server authentication.

   If SQL Server authentication is selected then enter the **Login ID** and **Password** in the fields provided.
2. Click **Next**.

If performing a dual-sided Application server installation you will be prompted for the following information for Side-B:

The **Side-B Management Portal Database Connection** dialog window is displayed.

1. In the **Side-B SQL Server** field enter the name of the SQL Server that the Unified Contact Center Management Portal Application is to connect to.
2. In the **Side-B Catalog Name** field enter the name of the database catalogue on the SQL Server.
3. In the **Connect Using** section, select the radio button of either:
   - Windows authentication, or
   - SQL Server authentication.

   If SQL Server authentication is selected then enter the **Login ID** and **Password** in the fields provided.
2. Click **Next**.

The **Side-A Reporting Services Connection** dialog window is displayed.

1. In the **Side-A Reporting Services Server** field, enter the web address of the Reporting Services server, which the Unified Contact Center Management Portal Application is to connect to.
2. Click **Next**.

If performing a dual-sided Application server installation you will be prompted for the following information for Side-B:

The **Side-B Reporting Services Connection** dialog window is displayed.

1. In the **Side-B Reporting Services Server** field, enter the web address of the Reporting Services server that the Unified Contact Center Management Portal Application is to connect to.
2. Click **Next**.

The **Ready to Install the Program** dialog window is displayed.

1. Click **Install**.

The **Installing Management Portal: Reporting Application Server** dialog window is displayed.

The **InstallShield Wizard Completed** dialog window is displayed.

1. Click **Finish**.

7. WEB SERVER COMPONENT

This chapter details how to install and configure the Unified Contact Center Management Portal Web Server components, including prerequisite software and the creation of user accounts.

Web Server Component Installation

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

1. If autorun is disabled and you have not been presented with the Unified Contact Center Management Portal Products Installation Application then double click the **autorun.bat** to launch the Unified Contact Center Management Portal installer.
2. Click the **Web Server** tab.

   The main panel is refreshed. A list of software applications that need to be installed before the Web component can be installed are displayed beneath the **Prerequisites** header. The following prerequisite applications are listed.

   - Windows Installer 3.1
   - Microsoft .NET Framework 2.0
   - ASP .NET State Service 2.0
3. Click the **Run Test…** button.

   The system checks if the above prerequisite applications are already installed.

   Any prerequisite application that is installed is displayed with a green tick next to it. Conversely, any prerequisite application that is not installed is displayed with a red cross next to it.

   Once all the prerequisite software is installed click the **Re-Run Test…** button to enable the **Install** button.
4. If all the prerequisite applications have a green tick displayed next to them, click the **Install** button to install the Web Server component.

The **Welcome to the Cisco Unified Communications** dialog window is displayed.

The **Welcome to the InstallShield Wizard: Management Portal Web Application** dialog window is displayed.

1. Click **Next**.

The **License Agreement** dialog window is displayed.

1. Select the **I accept the terms in the License Agreement** checkbox.
2. Click **Next**.

The **Ready to Install the Program** dialog window is displayed.

1. Click **Install**.

The **Installing Management Portal: Web Server** dialog window is displayed. During the installation command windows will be displayed whilst the configuration of Microsoft IIS is performed. These command windows will close by themselves once their tasks have completed. It is important not to interfere with this process.

The **InstallShield Wizard Completed** dialog box is displayed.

1. Click **Finish**.

Once the web server component has been installed, the following post installation steps are required for Internet Information Services.

In your Windows desktop, click **Start** > **Control Panel** > **Administrative Tools** and then double click **Internet Information Services (IIS) Manager**.

The **Internet Information Services (IIS) Manager** is displayed.

1. Expand the tree on the left and open the **Web Sites > Default Web Site** branch.
2. Right click the **Reports** virtual directory and click **Properties**.

The **Report Properties** dialog window is displayed.

1. Open the **ASP.NET** tab.
2. Click the **ASP.NET version** drop down list and select **1.1.4322**.
3. Click **Apply**.
4. Click **OK**.

Repeat the above steps for the **ReportServer** virtual directory.

8. PROVISIONING SERVER COMPONENT

This section describes guidelines for installing the Unified Contact Center Management Portal Provisioning component.

Provisioning Server Component Installation

Note: The Provisioning Server component is always installed on the server(s) hosting the Database component.

Note: Microsoft Message Queuing MSMQ should be installed prior to installation of the Provisioning Server component. In your Windows desktop click **Start** > **Control Panel** > **Add/Remove Programs > Windows components**. It appears as a sub-component of the **Application Server** Component. Install MSMQ in *workgroup mode* with **only** the common option selected. It is essential that the **Active Directory Integration** option is not selected.

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

1. If autorun is disabled and you have not been presented with the Unified Contact Center Management Portal Products Installation Application then double click the **autorun.bat** to launch the Unified Contact Center Management Portal installer.
2. Click the **Provisioning Server** tab.

   The main panel is refreshed. A list of software applications that need to be installed before the Provisioning component can be installed are displayed beneath the **Prerequisites** header. The following prerequisite applications are listed.

   - Windows Installer 3.1
   - J2SE Runtime Environment 5.0
   - MSXML 4.0 SP2 Parser
3. Click the **Run Test…** button.

   The system checks if the above prerequisite applications are installed.

   Any prerequisite application that is installed is displayed with a green tick next to it. Conversely, any prerequisite application that is not installed is displayed with a red cross next to it.

   Once all the prerequisite software is installed click the **Re-Run Test…** button to enable the **Install** button.
4. If all the prerequisite applications have a green tick displayed next to them, click the **Install** button to install the Provisioning Server component.

Caution: To install the Unified Contact Center Management Portal Provisioning component, you must have Administrator rights to the target server and

advanced user rights for *Logon as a service*. If your computer is connected to a network, network policy settings may prevent you from completing this procedure.

The **Welcome to the Cisco Unified Communications** dialog window is displayed.

The **Welcome to the Installshield Wizard for Management Portal: Provisioning Server** dialog window is displayed.

1. Click **Next**.

The **License Agreement** dialog window is displayed.

1. Select the **I accept the terms in the License Agreement** checkbox.
2. Click **Next**.

The **Customer Information** dialog window is displayed.

1. Enter the **User Name** and **Organisation** fields.
2. Ensure the **Anyone who uses this computer (All Users)** is selected.
3. Click **Next.**

The **Database Server** dialog window is displayed.

1. Select the required SQL Server from the **Database Server** drop down list. By default this will be **(local)** for the local machine.
2. Under **Connect Using**, select the checkbox of the connection method to be employed:
   - Windows authentication.
   - SQL Server authentication.

   If SQL Server authentication is selected then enter the **Login ID** and **Password** in the fields provided.
3. Click **Next**.

The **Ready to Install the Program** dialog window is displayed.

1. Click **Install**.

The **Installing Management Portal: Provisioning Server** dialog window is displayed.

The **InstallShield Wizard Complete** dialog window is displayed.

1. Click **Finish**.

Provisioning Component Configuration

Please see chapter 11.

9. DATA IMPORT SERVER COMPONENT

Data Import Server Component Installation

Install the Data Import Server component on the server hosting the Database Component.

To install the Unified Contact Center Management Portal Data Import Server component, perform the following:

1. If autorun is disabled and you have not been presented with the Unified Contact Center Management Portal Products Installation Application then double click the **autorun.bat** to launch the Unified Contact Center Management Portal installer.
2. Click the **Data Import Server** tab.

   The main panel is refreshed. The software application that needs to be installed before the Data Import component can be installed is displayed beneath the **Prerequisites** header. The following prerequisite applications are listed.

   - Windows Installer 3.1
   - Microsoft .NET Framework 2.0
3. Click the **Run Test…** button.

   The system checks if the above prerequisite application is installed.

   Any prerequisite application that is installed is displayed with a green tick next to it. Conversely, any prerequisite application that is not installed is displayed with a red cross next to it.

   Once all the prerequisite software is installed click the **Re-Run Test…** button to enable the **Install** button.
4. If all the prerequisite applications have a green tick displayed next to them, click the **Install** button to install the Data Import Server component.

The **Welcome to the Cisco Unified Communications** dialog window is displayed.

The **Welcome to the InstallShield Wizard for Management Portal: Data Import Server** dialog window is displayed.

1. Click **Next**.

The **License Agreement** dialog window is displayed.

1. Click the **I accept the terms in the license agreement** checkbox.

2. Click **Next**.

The **Cryptography Configuration** dialog window is displayed.

1. Enter the cryptographical pass phrase in the field provided.

Note: This must be the same passphrase created during the installation of the Application Server component.

2. Click **Next**.

The **Configure Database** dialog window is displayed.

1. In the **SQL Server** field enter the details of the SQL server machine.
2. In the **Catalog Name** field enter the name of the database as defined during the install of the Database Component.
3. In the **Connect Using** panel, select whether to use **Windows Authentication** or **SQL Server authentication**.
4. If you select the SQL Server option enter the **Login ID** and **Password** in the fields provided.
5. Click **Next**.

The **Ready to Install the Program** dialog window is displayed.

1. Click **Install**.

The **Installing Management Portal: Data Import Server** dialog window is displayed.

The **InstallShield Wizard Completed** dialog window is displayed.

1. Click **Finish**.

10. PRODUCT DOCUMENTATION

This chapter details the installation of the prerequisite software required to view the documentation supplied on the Unified Contact Center Management Portal CD.

Overview

The Unified Contact Center Management Portal is delivered with all the documentation you need to install, configure and use it. The documents are supplied in the Adobe PDF format. You will need to install the Adobe Acrobat Reader 7.0.

Documentation Installation

Open the Unified Contact Center Management Portal CD.

Select each manual and copy them to your preferred drive.

11. COMPONENT CONFIGURATION

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.

Database Component Configuration

Database Server Security Configuration

To configure database server security logon to the database server as a domain user with local administrative privileges. Open the **SQL Server Enterprise Manager**, click **Start** > **All Programs** > **Microsoft SQL Server** > **Enterprise Manager**.

The **SQL Server Enterprise Manager** is displayed.

Expand the tree of the appropriate database on the left of the screen. Click the **Security** folder, then the **Logins** folder. Right click on the main screen panel and select **New Login** from the drop down list.

The **SQL Server Login Properties – New Login** dialog window is displayed.

1. Add SQL logins for each Unifed Contact Center Management Portal web server hosting the Unified Contact Center Management Portal Web Server in this installation by typing the user as follows:
   - Under the **General** tab in the **Name** field enter the following: <DOMAIN>\<WEBSERVERMACHINENAME>$, for example, CISCODOM\UCCMPWEBA$. [This example configures access for the NETWORK SERVICE account from UCCMPWEBA].
   - Under the **Database Access** tab, select the **Portal** database checkbox and grant the above user the following roles by checking the appropriate checkboxes:
     - Public
     - portalapp_role
     - portalrs_role
     - portalreporting_role
2. Under the **Logins** section of SQL Server Enterprise Manager select the **NT AUTHORITY\NetworkService** user. Under the **Server Roles** tab check the box for the **Bulk Insert Admins** role.

Provisioning Server Component Configuration

To use the Provisioning Server monitoring utility ASP will need to be enabled on the machine(s) running the Unified Contact Center Management Portal Provisioning Server. To enable ASP in IIS, click **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

The **Internet Information Services (IIS) Manager** is displayed.

1. Click the **Web Service Extensions** folder.
2. Select the **Active Server Pages** extension from the list to the right.
3. Right click and select the **Allow** button. The status of the extension is changed to **Allowed**.

Note: If the ASP extension is already set to **Allowed**, leave the setting as it is.

Platform Server Cluster Configuration

Large deployments may require multiple servers to host the Unified Contact Center Management Portal platform to improve performance or data security. The platform hosts are connected together as a server *cluster*. This chapter details how to configure the Unified Contact Center Management Portal server cluster and data replication.

The Cluster Configuration Manager is a Unified Contact Center Management Portal client application that is used to configure server clusters, consisting of RDBMS databases, Report servers, Cisco ICM's and Call Managers. It is also used to replicate data between multiple Unified Contact Center Management Portal databases.

Configuration Overview

It is important that you configure the server cluster in the correct order. The configuration procedure is as follows.

Note: In a replicated environment you will only run this application on the **Side-A Database server**.

1. In the **Cluster Configuration Manager** server tab you will need to input the list of servers.
2. In the appropriate tab, you will need to enter the configuration data for the following:
   - The **Portal Server(s)** – the details of the server(s) containing the Unified Contact Center Management Portal database(s).
   - The **NAM(s)** – the details of the server(s) hosting NAM(s) and the database credentials for accessing thier data.
   - The **CICM(s)** – the details of the server(s) hosting the ICM and the database credentials for accessing their data.
3. The **Call Manager(s)** – the details of the server(s) hosting the Call Manager, the endpoint and security credentials for accessing the AXL interface.

Common ConAPI Credentials

For each CICM 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. Application instances may be created by running Cisco Configuration Manager on the CICM server. The Configuration Manager is usually located under **Program Files > ICM Admin Workstation** on the start menu of the ICM server. Once opened, launch the **Application Instance List** tool by locating it in the tree and double clicking on it.

Click the **Retrieve** button and the list of configured application instances are displayed. An application instance from this list may be used for the Unified Contact Center Management Portal or a new one can be created. The **Name** and **Application Key** fields displayed in the Cisco user interface map directly to the **Application Name** and **Application Key** fields in the Unified Contact Center Management Portal Cluster Configuration Manager. The name and key should be noted down for use during the configuration stage.

CMS Server Setup

Before configuring the Unified Contact Center Management Portal server cluster you must ensure that the CMS Server(s) are configured correctly on the CICM(s) being configured. The ICM Setup program on the CICM (**Program Files** > **ICM Admin Workstation** > **Setup**) provides the ability to select the **CMS Node** option when configuring Admin Workstations. CICM setup is outside the scope of this document but you must ensure that this option was selected. You can determine if the option has been selected by looking for a **cmsnode** and **cms_jserver** process running on the CICM.

A new application connection must be defined on each configured CICM for the Data Import Server. This can be achieved by running the CMS Control application on the CICM. CMS Control can be found under **Program Files** > **ICM Admin Workstation** on the start menu of the CICM being configured.

Click on the **Add** button to the right hand side of the screen to launch the **Application Connection Details** dialog window.

A new connection should be created with the following:

FIELD	VALUE	EXAMPLE
ICM Distributor AW link	*<Data Import Server Name>*Server	UCCMPServer
ICM Distributor AW RMI registry port	2099	2099
Application link	*<Data Import Server Name>*Client	UCCMPClient
Application RMI	2099	2099

registry port		
Application host name	*<Data Import Server Name>* or IP Address	UCCMP

Note: Where *<Data Import Server Name>* is defined, this should be replaced with the capitalised name of the Unified Contact Center Management Portal Data Import Server which is being configured to connect with the CICM.

Configuration Procedure

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

1. Navigate to the **Start > All Programs > Management Portal > Data Import Server** and click the **Cluster Configuration** application.

The **Connect to SQL Server** dialog window is displayed.

2. Select the required **Database** from the drop down list. This will be the database that was installed during the Database Component stage of the installation. The default value is **Portal.**
3. Select the **Use Integrated Security** checkbox.
4. Click **OK**.

The **Cluster Configuration Manager** user interface is displayed. When using integrated security the user running the **Cluster Configuration** application must have sufficient rights to execute SQL on the database server on which the application is running.

The interface consists of the following tabs. Click on the tab to display the tab contents:

Tab 1 – Servers

Note: This tab contains a list of all the servers in the cluster. Before a server is configured for a specific role e.g. NAM, ICM it must be configured here.

1. Click the **Servers** tab. A table is displayed with three columns:
   - **Server Name** – a name to refer to the server as. This is not necessarily the physical name of the server.
   - **Default Hostname** – the physical name of the server. The server must be accessible using this name from all machines in the cluster.
   - **Default IP Address** – the IP address of the server.
2. To add a new server to the cluster click **New**.

   The **Server Configuration** dialog window is displayed.
3. In the **Server Name** field enter the name of the server. This is a label to identify the machine in the cluster of servers.

4. In the **Default Hostname** field enter the name of the physical name of the machine. The machine should be accessible using this host name from anywhere in the cluster.
5. In the **Default IP Address** field, enter the IP address of the server.
6. Click **OK**.

The above steps should be repeated for all Unified Management Contact Center Management Portal Servers, ICM Servers, Call Manager Servers and NAM Servers in this installation.

Tab 2 – Portal Databases

This is used to configure relational databases.

1. Click the **Portal Databases** tab. A table is displayed with four columns:
   - RDBMS Server
   - RDBMS Catalog
   - OLAP Server
   - OLAP Catalog

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.

2. To create a new portal database server click **New**.

   The **Portal Database Configuration** dialog window is displayed.
3. Select the **RDBMS Server** from the drop down list.
4. Enter the **RDBMS Catalog** name in the field provided.
5. Click **OK**.

Note: Once the database(s) have been setup, you can configure replication. It is recommended that replication be confuigured before Network Application Managers (NAMs), Cisco Intelligent Call Managers (CICMs) and Call Managers are added to the cluster. For more information on how to configure replication see below.

Tab 3 – Report Server Databases

There is no current requirement to configure report servers in this version.

Tab 4 – NAM Databases

This is used to configure servers hosting Network Application Managers (NAMs).

1. Click the **NAM** tab.

   A table is displayed with seven columns:
   - **Instance Name** – the label used to identify the instance of the NAM in the cluster configuration tool.

- **Side-A Server** – the server that is hosting side-A of the NAM.
- **Side-A AWDB** – the database on the NAM that containes the side-A NAM's real-time data. Please take care to ensure that the case of the database name matches that on the NAM.
- **Side-A HDS** - the database on the NAM that containes the side-A NAM's historical-time data. Please take care to ensure that the case of the database name matches that on the NAM.
- **Side-B Server** – the server that is hosting side-B of the NAM.
- **Side-B AWDB** – the database on the NAM that containes the side-B NAM's real-time data. Please take care to ensure that the case of the database name matches that on the NAM.
- **Side-B HDS** - the database on the NAM that containes the side-B NAM's historical data. Please take care to ensure that the case of the database name matches that on the NAM.

2. To create a new NAM instance click the **New** button.

The **NAM Configuration** dialog window is displayed.

1. In the **Instance Name** field enter the name to represent the NAM instance.
2. Select the ICM version number from the **Version** drop down list.

In the **Side-A Servers** panel perform the following:

1. Select the **Server** from the drop down list that is hosting the NAM.
2. In the **AWDB Catalog** field enter the name of the AWDB catalog.
3. In the **HDS Catalog** field enter the name of the HDS catalog.

In the **Common Connection Parameters** panel, perform the following:

1. Select the **Windows authentication** radio button.
2. If the NAM Database is part of a dual sided configuration, select the **Dual Sided** checkbox and proceed to fill out the Side-B details as for Side-A above.

In the **Common ConAPI Credentials** panel, perform the following:

1. Enter the application name and application key of the application instance created on the ICM in the spaces provided. This is the

information gathered in the **Common ConAPI Credentials** section above.

2. Click **OK**.

   The above details populate the tab table fields.

3. Click the **Active Directory Mapping** button. This is used to provision domain users who are required for supervisor memberships. The domain user must first be a member of the domain active directory before managing resources.

The **Browse Active Directory** dialog window is displayed.

In the **Domain Settings** panel enter the following:

1. In the **Domain Controller A** field enter the name of the Domain Controller. (The **Domain Controller B** field is inactive).
2. Select the **Use Secure Authentication** checkbox.
3. In the **Username** field enter the name of the domain user.
4. In the **Password** field enter the domain user's password.
5. Click the **Refresh** button.
6. Select the **Active Directory** folder to use for LDAP account selection.
7. Click **OK**.

Tab 5 – CICM Databases

This is used to configure the Cisco Intelligent Call Managers (CICMs).

1. Click the **CICM** tab.

   A table is displayed with seven columns:

2. **Instance Name** – the label used to identify the instance of the CICM in the cluster configuration tool.
3. **Side-A Server** – the server that is hosting side-A of the CICM.
4. **Side-A AWDB** – the database on the instance name that contains the side-A CICM real-time data. Please take care to ensure that the case of the database name matches that on the ICM.
5. **Side-A HDS** - the database on the instance name that contains the side-A CICM's historical data. Please take care to ensure that the case of the database name matches that on the ICM.
6. **Side-B Server** – the server that is hosting side-B of the CICM.
7. **Side-B AWDB** – the database on the name that contains the side-B CICM's real-time data. Please take care to ensure that the case of the database name matches that on the ICM.
8. **Side-B CICM** - the database on the name that contains the side-B CICM's historical data. Please take care to ensure that the case of the database name matches that on the ICM.

9. To create a new ICM instance, click the **New** button.

The **CICM Database Configuration** dialog window is displayed.

1. In the **Instance Name** field enter the name of the CICM instance. This is a label for the ICM instance and is what will be used to reference the CICM in the cluster management utility.
2. Select the CICM version number from the **Version** drop down list.

In the **Side-A Servers** panel perform the following:

1. Select the **Server** from the drop down list that is hosting the CICM.
2. In the **AWDB Catalog** field enter the name of the AWDB catalog.
3. In the **HDS Catalog** field enter the name of the HDS catalog.

In the **Common Connection Parameters** panel, perform the following:

1. Select the **SQL Server authentication** radio button.
2. In the **Login Name** field enter the login name.
3. In the **Password** field enter the required password.

In the **Common ConAPI Credentials** panel, perform the following:

1. Enter the **application name** and **application key** (of the Application instance created on the ICM) in the fields provided. This is the information gathered in the **Common ConAPI Credentials** section above.
2. Click **OK**.
3. If the ICM instance is a NAM (an ICM that controls other CICMs) then select the **NAM Based** checkbox.
4. If the CICM instance belongs to a dual sided ICM configuration select the **Dual Sided** checkbox.

   The above details populate the tab table fields.
5. Click the **Active Directory Mapping** button. This is used to provision domain users who are required for supervisor memberships. The domain user must first be a member of the domain active directory before managing resources.

The **Browse Active Directory** dialog window is displayed.

In the **Domain Settings** panel enter the following:

1. In the **Domain Controller A** field enter the name of the Domain Controller. (The **Domain Controller B** field is inactive).
2. Select the **Use Secure Authentication** checkbox.
3. In the **Username** field enter the name of the domain user.
4. In the **Password** field enter the domain user's password.
5. Click the **Refresh** button.

6. Select the **Active Directory** folder to use for LDAP account selection.
7. Click **OK**.
8. Click **OK**.
9. Click **Apply**.
10. When prompted click **Yes** to apply your changes.

Tab 6 – CallManagers

If you are to configure CallManagers you must stop the **Management Portal Data Import** service before running the Cluster Configuration Manager. To do this proceed as follows leaving the Cluster Configuration Application open:

1. In your Windows desktop, click **Start** > **Run**.

The **Run** dialog window is displayed.

3. In the **Open** field, enter **services.msc**.

The **Services** dialog window is displayed.

1. Right click on the **Management Portal Data Import** service from the list of services.
2. Select **Stop**.
3. Close the Services dialog window.

Return to the Cluster Configuration Application to begin the configuration of the Call Manager(s).

1. Click the **CallManagers** tab.

   A table is displayed with two columns:

   - **Instance Name** – the name associated to the Call Manager instance. This is a display label that represents the related Call Manager.
   - **Endpoint URL** – The URL used to access the Call Manager AXL interface.
2. To add a Call Manager click **New**.
3. When prompted to import the Tenant/Peripheral data click **Yes**.

Note: The Tenant/Peripheral data import is a mandatory step during the initial configuration (this will fail if you have not stopped the data import service).

The **Configure CallManager** dialog window is displayed. A folder tree is displayed in which the call manager and tenants are displayed as folders.

1. In the **Peripheral Associations** panel, select the **CICM instance** from the drop down list that owns the CallManager to be configured.
2. Once selected, the **Select Peripherals** button becomes active. Click this button to display the **Peripherals Association** dialog window, which displays all the peripherals associated with the database.
3. Select the checkbox of the required peripherals and then add the name of the peripheral gateway user in the corresponding **PG User** field. The **PG User** is the directory user on the CallManager that new phones will be associated with when they are created through the Unified Contact Center Management Portal user interface. In order for the CICM to control the new phone it must be added to a specific users list of controlled devices in the directory on the CallManager. The user name entered here is the names that will be used for associating new phones.
4. Click **OK**.
5. Select the associated tenant from the folder tree. This will associate the Call Manager to the tenant to which it belongs.

In the **Call Manager Connection Details** section enter the following details:

1. In the **Instance Name** field enter the name of the Call Manager instance. This is a display only label that is used to refer to the Call Manager from within the Management Portal Cluster Management utility.

Note: It is recommended that it should match the appropriate CICM instance name.

2. In the **Server** drop down list, select the server hosting the Call Manager.
3. In the **Version** drop down list select the required Call Manager version.
4. In the **Endpoint** field confirm the URL is correct for the appropriate Cisco's CallManager web service. If not then enter the correct URL.
5. In the **User Name** field enter the name of the CCM Administrator user. This is the user name for the connection details to use when connecting to the Call Manager's web service. This is the Windows user (version 4x) or Linux user (version 5x) that will be authenticated against when a request is made to the CallManager.
6. In the **Password** field enter the CCM Administrator user's password. This is the password for the associated user entered in the previous step.
7. Click the **Test Connection** button to test the connection to the configured CallManager.

Note: The following two steps are not available during the initial configuration. These can be selected once the import process has been successful.

8. In the **Default Device Pool** drop down list select the preferred device pool to which IP Phones should be added by the Unified Contact Center Management Portal.
9. In the **Default Route Partition** drop down select the required route partition to which IP Phones should be added by the Unified Contact Center Management Portal.
10. Click **OK**.
11. Click **Apply**.
12. Click **Yes** to apply your changes.
13. Click **Close** to close the Cluster Configuration Manager.

Note: Once you have configured the CallManagers remember to restart the Management Portal Data Import service.

Data Replication

Required Account

The installation requires one domain user account (SQLAgentStart), which is used by SQL Server to replicate data between SQL Server databases:

Note: This user account can be any name, but we recommend SQLAgentStart. If you use a different account then please use your chosen user name wherever the SQLAgentStart User is referenced.

1. Create the SQLAgentStart Account; **<DOMAIN>\SQLAgentStart**.
2. SQLAgentStart requires *log on as a service* and *SQL Server administrative* privileges on the RDBMS servers.
3. Set the following attributes for this account:
   - Password never expires.
   - User cannot change password.

Where this account is used for database access some configuration is required after the relevant databases have been installed.

Configuring the SQLAgentStart Service

On the web and database component servers, give the SQLAgentStart user **System Administrator** privileges and then change the SQLAgentStart service to use the SQLAgentStart user.

Add the SQLAgentStart user to SQL Server logins and give the SQLAgentStart user access to the Unified Contact Center Management Portal database with the **db_datawriter** and **db_datareader** roles.

You must then logout of Windows and login as the new SQLAgentStart user. Then perform the following:

1. Create a linked server on the publisher (side A) machine pointing to the subscriber (side B) database.
2. On the subscriber (which is also the *distributor*), locate the **ReplData** folder (This is configured in SQL Server, by default this can be found in C:\Program Files\Microsoft SQL Server\MSSQL). Create a share for this folder with **Full Control** for Everyone.
3. Check that this share is accessible from the publisher while logged on as the SQLAgentStart 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 **Tab 1 – Servers** above, in the **Platform Server Cluster Configuration** section. Please note however that the first server setup is automatically the publisher. Subscribers can then be setup on alternative servers or as a logical partition on the publisher server.

Note: The user running the **Cluster Configuration Manager** requires administrative privileges to connect to both publisher and subscriber servers using *Windows Authentication* and also requires access to the Unified Contact Center Management Portal database. This is because the **SQLServerAgent** startup account requires low level privileges to perform replication.

1. Give this domain account **db_owner** access to the Portal database on both the Publisher and Subscriber.
2. Test the connectivity between both machines. Login to both sides using the above domain account and test whether you can connect to SQL Server (from both sides) using *Windows Authentication*.
3. Now log back onto both machines as the **domain administrator**.
4. Open the **Cluster Configuration Manager** user interface on the Publisher side. (See the previous sub section **Configuration Procedure** on page 41).
5. Click the **Portal Databases** tab.
6. Click **New**.

The **Portal Database Configuration** dialog window is displayed.

7. Select the **RDBMS Server** from the drop down list to be the subscriber.

8. Enter the **RDBMS Catalog** name in the field provided.

Note: The catalog name selected must be the same catalog name as used by the publisher.

1. Click **OK**. The configured subscriber is now displayed in the **RDBMS Server** column beneath the title **Subscriber**.
2. 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.

1. Click **OK**.
2. Click **Apply**.
3. Click **Replication** again.
4. Click **Replicate**.

The **Cisco Database Replication Configuration** dialog window is displayed again.

1. Click the **Replicate** button.

The **Confirm** dialog window is displayed.

1. Click **OK**.

The **Cisco Database Replication Configuration** dialog window is displayed.

1. Click **OK**.
2. In the **Cluster Configuration Manager** user interface, on the **Portal Databases** tab, click **Apply**, then **Close**.
3. Now log onto the Subscriber and open the **SQL Server Enterprise Manager**, then open the **Replication Monitor**. There are three publications with one snapshot agent per publication. Start the snapshot agent by right clicking on the agent and select **Start Agent** for the *Base* publication and then wait for the snapshot to finish before starting the next snapshot in the same manner.
4. Close the SQL Server Enterprise Manager.

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:

1. Make a note of the **Host Name** and **IP Addresses** of ALL of the machines that are hosting CVP.
2. Make a note of the **User Name** and **Password** of an administrative user on the domain so that you can configure *File Replication* and the *Distributed File System*.
3. Ensure that the **Distributed File System**, **File Replication** and **Remote Proceedure 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 using 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.

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

It may be required for redundancy build in to the CVP file upload solution. If this is the case then DFS shares should be setup on all the machines to which the media files should be copies and file replication enabled between 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 using 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.

6. The **Configure Replication Wizard** is displayed.
7. When prompted to select the initial master select the share located on the domain controller.
8. Select the **Full Mesh** topology for the replication set.
9. Finnaly 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

Done	Description
❑	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** area, click **Settings**. The **Startup and Recovery** dialog box is displayed. 4. In the **System startup** area, 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. Reboot for the changes to take effect.
❑	Defragment the page file and registry hives using http://www.sysinternals.com /Utilities /PageDefrag.html
❑	For the IIS DefaultAppPool: disable **IIS6 App Pool Shutdown**
❑	Modify machine.config: set maxconnection to 12 * # of CPUs. Machine.config can be found in C:\WINDOWS \Microsoft.NET \Framework \v1.1.4322 \CONFIG
❑	Modify machine.config: set maxIoThreads to 100
❑	Modify machine.config: set maxWorkerThreads to 100
❑	Modify machine.config: set minFreeThreads to 88 * # of CPUs
❑	Modify machine.config: set minLocalRequestFreeThreads to 76 * # of CPUs
❑	Modify Cisco web.config: set lowPoolInitialThreadCount to 5 Web.config can be found in C:\Program Files \Cisco \web
❑	Modify Cisco web.config: set lowPoolMaxThreadCount to 18
❑	Modify Cisco web.config: set lowPoolDynamicThreadTrigger to 400

❑	Modify Cisco web.config: set lowPoolDynamicThreadDecayTime to 300000
❑	Modify Cisco web.config: set lowPoolRequestQueueLimit to -1 (minus one)
❑	Modify Cisco web.config: set highPoolInitialThreadCount to 1
❑	Modify Cisco web.config: set highPoolMaxThreadCount to 2
❑	Modify Cisco web.config: set highPoolDynamicThreadTrigger to 250
❑	Modify Cisco web.config: set highPoolDynamicThreadDecayTime to 300000
❑	Modify Cisco web.config: set highPoolRequestQueueLimit to -1 (minus one)
❑	Modify Cisco web.config: set responseBufferSize to 8192
❑	Edit RSReportServer.config: set MaxActiveReqForOneUser = 100 RSReportServer.config can be found in C:\Program Files \Microsoft SQL Server \MSSQL \Reporting Services \ReportServer
❑	Edit RSReportServer.config: 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

Done	Description
❑	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

12. POST INSTALLATION STEPS

Report Uploading

Any report template that has not been created by the Unified Contact Center Management Portal platform will require importing into the system. The report template will be saved to a default folder that the upload report function is linked to, so the user does not need to browse to the folder in question.

To upload the report into the Unified Contact Center Management Portal system, perform the following:

In your Wndows desktop, click **Start** > **All Programs** > **Management Portal** > **Audit Reports** > **Audit Report Uploader**.

The **Upload Audit Reports** dialog window is displayed.

1. Enter the Administrator user in the **User Name** field.
2. Enter your Administrator password in the **Password** field.
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.

13. PLATFORM UNINSTALLATION

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

Uninstalling Provisioning Server Component

This process will remove the Provisioning Server component removing the Unified Contact Center Management Portal connection for any remote datasources. E.g. ICM, Call Manager.

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.

A dialog window is displayed asking you if you are sure that you wish to remove the **Management Portal: Provisioning Server**.

1. Click **Yes**.

The **Setup Status** dialog window is displayed. The extent of the un-installation progress is displayed on the progress bar.

Once completed, you will be prompted to re-start the system.

1. Click **Yes** to complete installation and restart the system.

Uninstallation of the Provisioning Server Component is complete.

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 e.g. ICM, Call Manager to the Unified Contact Center Management Portal datamart.

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

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

1. Click **Yes**.

The **Setup Status** dialog window is displayed. The extent of the un-installation progress is displayed on the progress bar.

Uninstallation of the Data Import Server Component is complete.

Uninstalling Database Component

This process will remove the database installation component, disable replication in a dual sided environment and remove the Unified Contact Center Management Portal database catalogs.

Note: Before un-installation proceeds it is recommended that you create a backup of the Unified Contact Center Management Portal database catalog. By default this catalog will be called **Portal**. In a replicated environment this backup should be taken from side-A.

If you have a dual-sided installation then you will need to perform the following process to remove replication. It is extremely important that these steps are successfully completed before you continue with un-installation.

1. Navigate to the **Start > All Programs > Management Portal > Data Import Server** and click the **Cluster Configuration** application.
2. Select the **Portal Databases** tab.
3. Click the **Replication** button.
4. Click the **Unreplicate** button to remove replication.

Note: Removing replication may take some time but is an important step in the un-installation process. Once replication has been successfully removed then you may proceed.

To remove the database catalog:

1. Navigate to the **Start > All Programs > Microsoft SQL Server** and click **Enterprise Manager**.
2. Select the Unified Contact Center Management Portal database to remove and press **delete**. This database is called **Portal** by default.
3. When asked to confirm this action click **Yes**.

Note: (If the database cannot be deleted because it is in use, right-click the **Portal** database and select **all tasks /detach database**, click the **Clear** button for **connections using this database**, accept the option to not inform users that their session has been terminated, then click the **Cancel** button. The database remains detached but connections currently using it

are cleared, which should allow it to be deleted. Perform the deletion quickly otherwise it may take multiple attempts.

The database setup application may now be removed.

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

1. Select **Management Portal: Database Setup**.
2. Click the **Remove** option.

A dialog window is displayed asking you if you are sure that you wish to remove the **Management Portal: Database Setup**.

1. Click **Yes**.

The **Setup Status** dialog window is displayed. The extent of the un-installation progress is displayed on the progress bar.

Uninstallation of the Database Component is complete.

Uninstalling Web Server Component

This process will remove the Web Server component. This will remove the user interface component that is used to add and manipulated data stored in the Unified Contact Center Management Portal datamart.

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

3. Select **Management Portal: Web Application**.
4. Click the **Remove** option.

A dialog window is displayed asking you if you are sure that you wish to remove the **Management Portal: Web Application**.

2. Click **Yes**.

The **Setup Status** dialog window is displayed. The extent of the un-installation progress is displayed on the progress bar.

Uninstallation of the Web Server Component is complete.

Uninstalling Application Server Component

This process will remove the Application Server component. This will remove the ability to communicate between the Web Application user interface and the Unified Contact Center Management Portal datamart.

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

1. Select **Management Portal: Reporting Application Server**.
2. Click the **Remove** option.

A dialog window is displayed asking you if you are sure that you wish to remove the **Management Portal: Reporting Application Server**.

1. Click **Yes**.

The **Setup Status** dialog window is displayed. The extent of the un-installation progress is displayed on the progress bar.

Uninstallation of the Application Server Component is complete.

Uninstalling Reporting Extensions Component

This process will remove the Reporting Extensions component. This will remove the ability run reports on the Unified Contact Center Management Portal platform.

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

3. Select **Management Portal: Reporting Extensions**.
4. Click the **Remove** option.

A dialog window is displayed asking you if you are sure that you wish to remove the **Management Portal: Reporting Extensions**.

2. Click **Yes**.

The **Setup Status** dialog window is displayed. The extent of the un-installation progress is displayed on the progress bar.

Note: In some circumstances un-installation may not be able to stop Microsoft Reporting Services in a timely fashion. If an error occurs during installation then you should check that the **ReportServer** service is stopped and then re-attempt un-installation. Once un-installation is complete the **ReportServer** service should be re-started.

Uninstallation of the Reporting Extensions Component is complete.

14. GLOSSARY

A

Adaptor – (See Connector)

Appender

A software tool which adds data to the end of a file.

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.

D

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.

E

Event Log

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

F

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.

G

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.

H

Handle

A pointer in programming, which enables the program to access a resource or function.

Hardening – (See Security)

A process or measure, which provides for or improves the security of your computer system.

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.

L

Logger

A software application, which logs events.

M

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.

P

Polling

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

R

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.

S

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.

T

Thread

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

U

Universal Naming Convention (UNC)

A PC format for specifying the location of resources on a local-area network (LAN).

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.

W

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.

Workflow

A defined series of tasks within an organization to produce a final outcome.

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.

15. INDEX

S

T

U

V

W