Installation Guide for Cisco Unified Contact Center Management Portal

Release 7.1(3)

December 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 (6387)
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”

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

Chapter 2, “Installation Guidelines”

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

Chapter 3, “Component Installation”

Provides instructions for the installation of all the Management Portal components.

Chapter 4, “Component Configuration ”

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

Chapter 5, “Post Installation Steps”

Describes how to set the administrator password for, and upload report templates into, the Unified Contact Center Management Portal platform.

Chapter 6, “Upgrading From a Previous Version”

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

Chapter 7, “Component Uninstallation”

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

Obtaining Documentation

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 Enterprise and Hosted Editions. The Unified Contact Center Management Portal serves three mutually supportive purposes:

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

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

Primary Functionality

- **Unified Configuration**, that is, tenant provisioning of both the applicable IPCC Enterprise Edition ICM, or 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

  These permissions are completely configurable

- **Audit Trails** on configuration changes and usage

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

- **Commissioning** consists of operations that install and initially configure a system of components. These operations are typically done by the Service Provider using existing setup and configuration tools. Examples include setting up and configuring CallManagers
- **Provisioning** consists of day to day configuration operations performed by a tenant. Examples include creating or modifying Agents, Skill Groups and Agent Teams

The Service Providers uses the existing IPCC Enterprise or Hosted Edition, CallManager and CVP tools (installers and configuration tools) to commission a system. They will then install the Unified Contact Center Management Portal Provisioning System and use it to define tenants and set up tenant permissions. Tenants may 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 Enterprise or Hosted Edition 7.1. It works with the standard IPCC Enterprise and Hosted Editions, and CallManager.

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

Additionally, the Unified Contact Center Management Portal system can read existing configuration data from IPCC Enterprise or Hosted Editions and CallManager, store it in the Unified Contact Center Management Portal database and reconcile differences between the two. This enables Service Providers to make configuration changes using existing IPCC Enterprise/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 Enterprise and Hosted Edition deployments with the following restrictions:

- Each Tenant must have its own:
  - ICM or 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 Enterprise and Hosted Editions 7.1 and above

Deployment Models

N-Sided Replication

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

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

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

- **Dedicated Server**. All the Unified Contact Center Management Portal components are installed on a single dedicated server. This system can manage **150 Portal users** concurrently
- **Secure Deployment**. The Unified Contact Center Management Portal Application, Web and Reporting components are hosted on one server and the Provisioning, Data Import and Database components are hosted on a second server. This system can manage **600 Portal users** concurrently

2. INSTALLATION GUIDELINES AND REQUIREMENTS.

General Advice

- Do NOT install the Unified Contact Center Management Portal platform on a domain controller
- 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)
- 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 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 Administration Guide for Unified Contact Center Management Portal Release 7.1(3))
- 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)
- 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, Cisco recommends that you 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 backup the SQL Server databases and truncate transaction logs to prevent them becoming excessively large
- Schedule backups for quiet times of the day

Security Guidelines

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

Windows Components

The following windows components are required for installation:

- **Microsoft Message Queuing**
- **Microsoft Windows 2003 Application Server with ASP.NET components (IIS)**
- **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. A mandatory check is performed before each part of the installation. If this check does not find the required software then the installation will refuse to proceed.

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

A summary of these prerequisites is listed below.

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

Database

- Windows Installer 3.1
- 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

Note Some Management Portal components require other Management Portal components to be installed first. It is therefore recommended that all components are installed in the order given in this Guide.

3. COMPONENT INSTALLATION

Planning Your Installation

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

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

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

Running the Installer

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

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

2. Clicking on a tab will bring up, in the main panel, the list of prerequisites for that component and the offer to check that those prerequisites are installed
3. It is recommended that you go through the installation of the components in the order given by this manual
4. To begin the installation of each individual component, click on its tab and click the **Run Test…** button to check that the listed prerequisite applications are installed. Only when the installer has verified the presence of these components will you be able to click the **Install** button to proceed with the installation of that component

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

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

Recording Your Settings

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

Management Portal		
Database Catalog Name		
Cryptographical Passphrase		
Administrator Password		
CICM/ICM	**Side A**	**Side B**
Application Name		
Application Key		
NAM	**Side A**	**Side B**
Application Name		
Application Key		

Note The cryptographical passphrase is a vital piece of information and must be recorded as it will be needed not only during the installation of both the Application Server and Data Import components, but also in any future installations (for example, when adding new servers to the cluster)

Database Component

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

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

1. Select the Database Component tab, click **Run Test…** to check for prerequisites (see page 21), and click **Install**. The **Welcome to the Cisco Unified Communications** dialog window is displayed. Click **Next** to go through each window in turn
2. On the **License Agreement** dialog window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting
3. Click **Install**

Note This does not install a new database component; it installs the database setup wizard.

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

When the InstallShield Wizard has completed, you can choose to install the database immediately or do so at a later date.

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

Note You must set up your database in order to complete the installation of all Management Portal components.

Database Setup

If you checked the **Launch Management Portal: Database Setup** checkbox after installing the Database component, the database setup wizard will launch automatically.

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

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

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

1. On the **License Agreement** dialog window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting
2. On the **SQL Server Connection Details** dialog window:
   - **Server Name** Select the SQL Server where the Unified Contact Center Management Portal database should be installed. In most cases this will be the machine running the application, in which case it should be left as the default **(local)**
   - **Database Name** Enter or select the name of the database catalog that will be used for Unified Contact Center Management Portal. It is recommended that you use the default name of **Portal**
   - **Connect Using** Select the radio button of the login credentials you wish to apply:
     - **Windows login credentials** This is the recommended option
     - **SQL Server login credentials** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your **Login Name** and **Password** in the fields provided
   - **Test Connection** Makes sure the connection to the SQL Server is established. The message 'Connection succeeded but database

does not exist' is correct behavior at this point. Click **OK** to continue

3. On the **Select an Action to Perform** dialog window:
   - **Install a new database** Installs a new database. You may maintain or delete a database by running the installer again and selecing the appropriate option
4. The fields on the **Configure the Location of Data Files** dialog window only need to be completed if you are using a custom installation of SQL Server. If you are not using a custom installation of SQL Server, ignore these fields
   - **Location** When you select a File Group(s), its location is shown in this field. To change this location, browse to the new location
   - **Initial Size** Select the space that should be allocated for this File Group(s). The default is 5MB
   - **Maximum Size** Set the storage capacity for the selected File Group(s). The default is 1000MB. You can also choose to set no limit to the file size by selecting the **Unrestricted Size** checkbox, though this is not recommended
   - **Update** Saves your changes to the selected File Group(s)
   - **Default** Returns the settings for all File Groups to their default
5. Confirm the details you have selected. If any of these details are incorrect, click **Back** to the appropriate stage to correct them.
6. Click **Next** to begin installation. Installation will take several minutes. A new window will appear to notify you when it is complete
7. Click **Close** to close the installer

Database Replication

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

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

Database Component Configuration

Please see chapter 4.

Reporting Extensions Component

This section details how to install and configure the Unified Contact Center Management Portal Reporting Extensions.

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. Select the Reporting Extensions Component tab, click **Run Test…** to check for prerequisites (see page 21), and click **Install**
2. On the **License Agreement** dialog window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting
3. Click **Install**
4. When the installation is completed, click **Finish**

Application Server Component

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

Application Server Component Installation

To install the Unified Contact Center Management Portal Application Server component, select the Application Server Component tab, click **Run Test…** to check for prerequisites (see page 21), and click **Install.**

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

1. On the **License Agreement** dialog window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting
2. On the **Cryptography Configuration** dialog window:
   - **Passphrase** Create a cryptographical pass phrase of between 6 and 35 characters. This passphase is used for encrypting and decrypting system passwords and must be the same for all servers in the cluster
   - **Confirm Passphrase** You will not be able to continue until the contents of this field are identical to the passphrase entered above

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

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

Tip You can create a password that is both memorable and secure by choosing a memorable phrase, selecting the first letters of each word in that phrase, and turning some of these letters into numbers. For example, the proverb 'a chain is no stronger than its weakest link' shortens to 'acinstiwl', which can be turned into a password 'AC1n5t1WL'.

3. On the **Application Server Location** dialog window:
   - **Side A / Side B / Standalone** Select the option that corresponds to the side which you are installing. If the Application Server is being installed on a single sided platform (one that uses one server for all components) select the **Standalone** option
4. On the **Side A Management Portal Database Connection** dialog window:
   - **Side A SQL Server** 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. The default is localhost
   - **Side A Catalog Name** Enter the name of the database, as selected in the Database Component installation (see page 23). By default this is **Portal**
   - **Connect Using** Windows authentication should be used in most cases. If the database server is on a different network, select SQL Server authentication and enter the appropriate **Login ID** and **Password** in the fields provided
5. If performing a dual-sided installation, you will also be presented with the **Side B Management Portal Database Connection** dialog window:
   - **Side B SQL Server** Enter the name of the side B server where the Unified Contact Center Management Portal database has been installed
   - **Side B Catalog Name** Enter the name of the database, as selected in the Database Component installation (see page 23). By default this is **Portal**
   - **Connect Using** Windows authentication should be used in most cases. If the database server is on a different network, select SQL Server authentication and enter the appropriate **Login ID** and **Password** in the fields provided
6. On the **Side A Reporting Services Connection** dialog window:
   - **Side A Reporting Services Server** Enter the web address of the Reporting Services server that the Unified Contact Center Management Portal Application Server is to connect to

Note The default value of localhost is valid only for a standalone installation.

7. If performing a dual-sided installation, you will also be presented with the **Side B Reporting Services Connection** dialog window:

- **Side B Reporting Services Server** Enter the web address of the Reporting Services server that the Unified Contact Center Management Portal Application Server is to connect to

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

Web Server Component

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

Web Server Component Installation

To install the Unified Contact Center Management Portal Web Server component, select the Web Server Component tab, click **Run Test…** to check for prerequisites (see page 21), and click **Install**.

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

1. On the **License Agreement** dialog window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting
2. Click **Install.** During the installation, command windows will be displayed while the installer configures Microsoft IIS. These command windows will close by themselves and require no action from you
3. When the installation is completed, click **Finish**

Configuring IIS

You must ensure that the version of ASP.NET used by Internet Information Services is set to version 1.1.4322, or audit reporting will fail. This may be performed either immediately following installation of the Web Server component, or at the end of the installation.

Note This step must be performed even when upgrading an existing version of the Management Portal, as the installation procedure will reset the ASP.NET version

1. In your Windows desktop, click **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**. The **Internet Information Services (IIS) Manager** is displayed
2. Expand the tree on the left and open the **Web Sites > Default Web Site** branch
3. Right click the **Reports** virtual directory and click **Properties**. The **Report Properties** dialog window is displayed
4. Open the **ASP.NET** tab

5. Click the **ASP.NET version** drop down list and select **1.1.4322**
6. Click **Apply**
7. Click **OK**

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

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 must always be installed on the server(s) hosting the Database component.

Caution You must have Administrator rights on 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.

To install the Unified Contact Center Management Portal Provisioning component, select the Provisioning Server Component tab, click **Run Test…** to check for prerequisites (see page 21), and click **Install**.

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

1. On the **License Agreement** dialog window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting
2. On the **Customer Information** dialog window:
   - **User Name** Your name or position
   - **Organisation** This is normally the company for which the Management Portal is being installed
   - **Anyone who uses this computer (All Users):** Ensure this box is checked before proceeding
3. On the **Database Server** dialog window:
   - **Database Server** Select the required SQL Server from the drop down list. By default this will be **(local)** for the current machine
   - **Connect Using** Select the radio button of the login credentials you wish to apply:
     - **Windows login credentials** This is the recommended option
     - **SQL Server login credentials** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your **Login Name** and **Password** in the fields provided

4. Click **Install**
5. When the installation is completed, click **Finish**

Provisioning Component Configuration

Please see chapter 4.

Data Import Server Component

Data Import Server Component Installation

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

To install the Unified Contact Center Management Portal Data Import Server component, select the Data Import Server Component tab, click **Run Test…** to check for prerequisites (see page 21), and click **Install**.

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

1. On the **License Agreement** dialog window:
   - **I accept the terms in the license agreement** You must select this option before you can continue. In doing so you agree to be bound by the terms in the license agreement, and so you should read it thoroughly before accepting
2. On the **Cryptography Configuration** dialog window:
   - **Passphrase** Enter the cryptographical passphrase you created during installation of the Application Server component
   - **Confirm Passphrase** You will not be able to continue until the contents of this field are identical to the passphrase entered above

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

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

Product Documentation

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

This documentation is supplied in PDF format. You must have the Adobe Acrobat Reader 7.0 or better installed in order to view it.

Documentation Installation

Open the Unified Contact Center Management Portal CD.

Select each manual and copy it to your preferred location.

4. 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

1. To configure database server security, logon to the database server as a domain user with local administrative privileges
2. Open the **SQL Server Enterprise Manager**, by clicking **Start** > **All Programs** > **Microsoft SQL Server** > **Enterprise Manager**. The **SQL Server Enterprise Manager** will be displayed
3. Navigate to the appropriate database server (in most cases this will begin with **(local)**) on the left of the screen
4. Open up the **Security** folder, and right-click on **Logins**
5. Select **New Login** from the drop down list. The **SQL Server Login Properties – New Login** dialog window is displayed
6. Add SQL logins for each server hosting the Unified Contact Center Management Portal Web Server in this installation by filling in the fields as follows:
   - **General** tab
     - **Name** Enter the machine name in the form <DOMAIN>\<WEBSERVERMACHINENAME>$, for example CISCODOM\UCCMPWEBA$. This configures access for the NETWORK SERVICE account from the web server machine
     - **Authentication** Select Windows Authentication unless connecting to a server on a different domain
   - **Server Roles** tab
     - **Server Roles** Check the box for the **Bulk Insert Administrators** role
   - **Database Access** tab
     - **Specify which databases can be accessed by this login** Select the checkbox for the Management Portal database (unless otherwise specified during installation this will be **Portal**)
     - **Database roles for 'Portal'** Grant the following roles to the login by checking the corresponding checkboxes:
       - Public

- portalapp_role
- portalrs_role
- portalreporting_role

7. Click **OK**
8. In the right-hand pane of the Enterprise Manager, right-click on the **NT AUTHORITY\NETWORK SERVICE** user and select **Properties** to edit it. Under the **Server Roles** tab check the box for the **Bulk Insert Administrators** role and click **OK**.

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:

1. Click **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**. The **Internet Information Services (IIS) Manager** is displayed
2. Navigate to and select the **Web Service Extensions** folder
3. From the list to the right, select the **Active Server Pages**
4. 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.

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 record the account used and substitute your chosen user name wherever the SQLAgentStart User is referenced.

1. Using Active Directory, create the SQLAgentStart Account **<DOMAIN>\SQLAgentStart**
2. Give SQLAgentStart the following privileges on the database 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

1. On the database servers, give the SQLAgentStart user **System Administrator** privileges by using the **Computer Management** tool to add the account to the Administrators group

2. Run services.msc, locate the SQLSERVERAGENT service and edit its proprties to use the <DOMAIN>\SQLAgentStart user
3. Open **SQL Server Enterprise Manager**, navigate to the Security folder, and add the SQLAgentStart user to SQL Server logins
4. On the Database Access tab, give the SQLAgentStart user access to the Unified Contact Center Management Portal database with the **db_datawriter** and **db_datareader** roles
5. Open the **Local Security Policy** tool to give the SQLAgentStart user **log on as a service** privileges
6. Log out of Windows and login as the new SQLAgentStart user
7. On the subscriber, locate the **ReplData** folder (this is configured in SQL Server, and by default can be found in C:\Program Files\Microsoft SQL Server\MSSQL). Create a share for this folder with **Full Control** for Everyone
8. 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
9. On the publisher, open the **SQL Server Query Analyzer** and check connectivity to side B using *Integrated Security*
10. 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 2 – Databases** on page 37.

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.

1. 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*.
2. Now log back onto both machines as the **domain administrator**

You are now prepared to set up replication as part of cluster configuration.

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 section 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 ICMs and CallManagers. It is also used to replicate data between multiple Unified Contact Center Management Portal databases.

Configuration Overview

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

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

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

In the **Cluster Configuration Manager** server tab you will need to input the list of servers, and the configuration data for each of the following in order:

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

Common ConAPI Credentials

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

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

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

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

2. Under **Tools/List Tools** you will find the **Application Instance List**. Double-click this to open it
3. Click the **Retrieve** button to display the list of configured application instances. You can use an application instance from this list for the

Unified Contact Center Management Portal or create a new one. To create a new application instance:

- Click **Add**, and enter the following details:
- **Name** A unique name to be used for the application instance
- **Application Key** A password to be used by the Portal to connect. This may be between 1 and 32 characters
- **Confirm Application Key** Ensure that no typographical errors were made while choosing the application key
- **Application Type** Select **<Other>**
- **Permission Level** Give the application **Full read/write** permissions

4. Record these details for use during the configuration of the cluster
5. Click **OK**

CMS Server Setup

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

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

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

A new application connection must be defined on each configured CICM or ICM for the Data Import Server. To do this:

1. Go to **Start > Program Files** > **ICM Admin Workstation > CMS Control** on the CICM or ICM being configured. This opens the CMS control console
2. Click on the **Add** button to the right hand side of the window to launch the **Application Connection Details** dialog window and fill in the fields as follows:
   - **ICM Distributor AW link** This should be the name of the Data Import server, with 'Server' appended, such as UCCMPServer
   - **ICM Distributor AW RMI registry port** Replace the default (1099) with 2099
   - **Application link** This should be the name of the Data Import server, with 'Client' appended, such as UCCMPClient
   - **Application RMI registry port** Replace the default (1099) with 2099
   - **Application host name** The server name or fixed IP address, such as UCCMP or 240.24.53.107

- Click **OK**, and **OK** again to save your changes and close the CMS control console

Configuration Procedure

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

1. Go to **Start > All Programs > Management Portal > Data Import Server > Cluster Configuration**
2. The **Connect to SQL Server** dialog window is displayed. On this window:
   - **Server Name** This option defaults to the current machine and cannot be changed
   - **Database** Select the Management Portal database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**
   - **Use Integrated Security** Ensure this option is checked
3. Click **OK** to open the **Cluster Configuration Manager**.

Note When using integrated security, the user running the **Cluster Configuration** application must have permission 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

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

1. Click the **Servers** tab. A table is displayed, with three columns, that will show information about the Servers once they have been configured
2. Click **New** to add a new server to the cluster. The **Server Configuration** dialog window is displayed

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

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

Note In some cases two or more of these fields may be identical

3. Click **OK**.

The above steps should be repeated for all Unified Management Contact Center Management Portal Servers, ICM Servers, CallManager Servers and NAM Servers (IPCC Hosted Edition only) 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, that will display information about the Databases once they have been configured
2. To create a new portal database server click **New**. The **Portal Database Configuration** dialog window is displayed

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

3. Enter the following details:
   - **RDBMS Server** Select the server that the database is installed on from the drop down list of the servers you configured on the **Servers** tab earlier. This defaults to the current machine
   - **RDBMS Catalog** Enter the name of the database in the field provided. This defaults to Portal

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

4. Click **OK**.

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

Replication

1. Click the **Replication** button. The **Cisco Database Replication Configuration** dialog window is displayed, in which all the selected server details are displayed. Perform any modifications at this stage if necessary
2. Click the **Replicate** button (if asked to save changes, click **OK**) and confirm
3. Click **OK** to close the Cisco Database Replication Configuration window
4. Click **Apply**, then **Close**
5. Now log onto the Subscriber and open the **SQL Server Enterprise Manager**, then open the **Replication Monitor**. Under **Agents/Snapshot Agents** three snapshot agents are listed
6. Start the first snapshot agent (that for the *Base* publication) by right clicking on the agent and selecting **Start Agent**. Wait for the snapshot

status to change to ‘succeeded’ (this may take several minutes) before starting the next snapshot in the same manner.

7. Close the SQL Server Enterprise Manager

Tab 3 – Report Server Databases

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

Tab 4 – NAM Databases

Note This tab is relevant to IPCC Hosted Edition only.

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

1. Click the **NAM** tab
2. A table is displayed, with seven columns, that will show information about the NAMs once they have been configured
3. To create a new NAM instance, click the **New** button. The **NAM Configuration** dialog window is displayed
   - **Instance Name** Enter a unique name to represent the NAM instance
   - **Version** Select the ICM version number from the drop down list
   - **Dual Sided** Check this box if you are using a dual-sided installation of the Management Portal. You will then be able to fill in details for Side B
   - **Server** Select the server that is hosting the NAM from the drop down list of the servers you configured on the **Servers** tab earlier
   - **AWDB Catalog** Enter the name of the administrative workstation database catalog, such as nam_awdb
   - **HDS Catalog** Enter the name of the historical data server catalog, such as nam_hds

Note If you do not know the names of the AWDB and HDS databases, you can find them using the ICMDBA utility, which is run from the command line prompt of the NAM server. Refer to the *ICM Administrator Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for information on how to use this utility.

- **Connect Using** Select the radio button of the login credentials you wish to apply:
  - **Windows login credentials** This is the recommended option
  - **SQL Server login credentials** This option should only be selected if you are using a database catalog on a different domain. For this option you must enter your **Login Name** and **Password** in the fields provided

- **Application Name** Enter the name of the application you created on the CICM/ICM earlier (see page 34)
- **Application Key** Enter the password of the application you created on the CICM/ICM earlier

4. Click the **Active Directory Mapping** button. The **Browse Active Directory** dialog window is displayed. This is used to provision the domain users who are required for supervisor memberships. The domain user must be a member of the domain active directory
   - **Domain Controller A** Enter the name of the Domain Controller
   - **Domain Controller B** Enter the name of the Side B Domain Controller if present
   - **Use Secure Authentication** Select this checkbox in order to login to the domain controller as a specified user
     - **Username** Enter the name of the domain user, such as NAMSERV\administrator
     - **Password** Enter the domain user's password
5. Click **Refresh**
6. Navigate to the **Active Directory** folder to use for LDAP account selection
7. Click **OK**, and **OK** again to save the new NAM

Tab 5 – CICM Databases

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

1. Click the **CICM** tab. A table is displayed, with seven columns, that will show information about the CICMs once they have been configured
2. To create a new CICM or ICM instance, click the **New** button. The **CICM Database Configuration** dialog window is displayed
   - **Instance Name** Enter a unique name to represent the CICM/ICM in the Management Portal
   - **Version** Select the CICM/ICM version number from the drop down list
   - **NAM Based** If the ICM instance is a NAM, then select the NAM Based checkbox
   - **Dual Sided** If the CICM/ICM instance belongs to a dual sided ICM configuration select the Dual Sided checkbox
   - **Server** Select the server that is hosting the CICM or ICM from the drop down list of servers you configured on the **Servers** tab earlier
   - **AWDB Catalog** Enter the name of the AWDB catalog, such as cicm_awdb

- **HDS Catalog** Enter the name of the HDS catalog, such as cicm_hds

Note If you do not know the names of the AWDB and HDS databases, you can find them using the ICMDBA utility

- **Connect Using** Select the radio button of the login credentials you wish the Data Import server to use.

Note As the Data Import Server service runs under a user who does not, by default, have administrator permissions, you should **not** use Windows authentication unless these defaults have been changed

- **Windows authentication** Select this option only if the Local System user has administrator permissions on the server the CICM is installed on, or if you have configured the Management Portal Data Import Server service to run under a different user that does have administrator permissions.
- **SQL Server authentication** Most installations should select this option. Enter the **Login Name** and **Password** in the fields provided
- **Application Name** Enter the name of the application you created on the CICM/ICM earlier (see page 34)
- **Application Key** Enter the password of the application you created on the CICM/ICM earlier

3. Click the **Active Directory Mapping** button. The **Browse Active Directory** dialog window is displayed. This is used to provision the domain users who are required for supervisor memberships. The domain user must be a member of the domain active directory
   - **Domain Controller A** Enter the name of the Domain Controller
   - **Domain Controller B** Enter the name of the Side B Domain Controller if present
   - **Use Secure Authentication** Select this checkbox in order to login to the domain controller as a specified user
     - **Username** Enter the name of the domain user, such as CICMSERV\administrator
     - **Password** Enter the domain user's password
4. Click **Refresh**
5. Navigate to the **Active Directory** folder to use for LDAP account selection
6. Click **OK**, and **OK** again to save the new CICM/ICM configuration

Tab 6 – CallManagers

You must stop the **Management Portal Data Import** service before configuring CallManagers. Leave the Cluster Configuration Application open, and:

1. In your Windows desktop, click **Start** > **Run**. The **Run** dialog window is displayed
2. In the **Open** field, enter **services.msc**. The **Services** dialog window is displayed
3. Locate the **Management Portal Data Import** service in the list of services
4. Right-click on the Management Portal Data Import service and select **Stop**

Note You may wish to leave this dialog window open to simplify restarting the process after CallManager configuration.

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

1. Click the **CallManagers** tab. A table is displayed, with two columns, that will show information about the CallManagers once they have been configured
2. To add a CallManager click **New**
3. When prompted to import the Tenant/Peripheral data click **Yes**

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

Note If the import is not complete within a few minutes, this may be because the Data Import service has not been stopped as described above

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

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

   - **Server** Select the server hosting the CallManager that you configured on the Servers tab earlier
   - **Version** Select the required CallManager version
   - **Endpoint** Enter the URL used to access the CallManager AXL interface. The default is the default URL for the CallManager version selected
   - **User Name** Enter the name of the CallManager Administrator user. This is the user name that the Management Portal Data Import Server will use when connecting to the CallManager's web service.
   - **Password** Enter the CallManager Administrator user's password
   - **Test Connection** Click to test the connection to the configured CallManager
5. Open up the tree on the left, and double click on a tenant name to bring up the **Peripheral Association** dialog box for that tenant

6. Select the checkbox of the required peripherals
   - **Peripheral User Name** Enter the name of a directory user on the CallManager, with whom new phones will be associated with when they are created through the Unified Contact Center Management Portal user interface. In order for the CICM/ICM to control the new phone it must be added to a specific user's list of controlled devices in the directory on the CallManager. You can find a list of directory users by logging into Cisco Unified CallManager Administration (normally https://<*SERVER*>/ccmadmin, for example https://CCMSERV ccmadmin).
7. Click **OK**
8. Select the associated tenant from the folder tree. This will associate the CallManager to the tenant to which it belongs

When you have finished adding CallManagers, restart the **Management Portal Data Import** service.

CVP Media File Upload

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

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

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

Preparing the Configuration

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

- Make a note of the **Host Name** and **IP Addresses** of ALL of the machines that are hosting CVP
- Make a note of the **User Name** and **Password** of an administrative user on the domain so that you can configure *File Replication* and the *Distributed File System*

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

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

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

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 to be built into 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 among all of them.

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

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

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

Performance Configuration Checklists

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

Web Server

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

5. POST INSTALLATION STEPS

Logging into the Management Portal

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

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

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

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

Report Uploading

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

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

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

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

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

3. Click **Upload**

The Report Uploader now transfers the report template from the folder in which it was installed to a shared folder for users to access.

6. UPGRADING FROM A PREVIOUS VERSION

This chapter details how to upgrade from Management Portal version 7.1(1) to version 7.1(3).

Overview

To upgrade the Management Portal, it is necessary to uninstall all of the components except for the Database Server component. The new version of the Management Portal is then installed, and your database upgraded.

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

Uninstallation

Run through the uninstallation procedure given in Chapter 7 Platform Uninstallation. **Do not uninstall the Database Compoment**. When this is done, instead of closing down the Add/Remove Programs window, you should also uninstall the Management Portal: Database Setup program.

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

Installation

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

Configuration

Click on **Start > All Programs > Management Portal > Data Import Server > Cluster Configuration** and check that the settings are correct. When you are satisfied run services.msc and check that the Management Portal Data Import Server service is started.

Replication

To set up replication on the upgraded system:

1. Open the Portal Databases tab on the **Cluster Configuration Manager**
2. Click **Replication** to open the **Cisco Database Replication Configuration** dialog window
3. Click the **Replicate** button and confirm
4. Click **OK** to close the Cisco Database Replication Configuration window

5. Click **Apply**, then **Close**
6. Now log onto the Subscriber and open the **SQL Server Enterprise Manager**, then open the **Replication Monitor**. Under **Agents/Snapshot Agents** three snapshot agents are listed
7. Start the first snapshot agent (that for the *Base* publication) by right clicking on the agent and selecting **Start Agent**. Wait for the snapshot status to change to 'succeeded' (this may take several minutes) before starting the next snapshot in the same manner.
8. Close the SQL Server Enterprise Manager

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

7. PLATFORM UNINSTALLATION

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

Uninstalling Data Import Server Component

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

Removing Replication

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

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

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

You may now remove replication.

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

Note Removing replication may take some time.

Once replication has been successfully removed then you may proceed.

Uninstalling Data Import Server Component

1. Insert the CD that came with your old version of the Management Portal. Close any windows that automatically open

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

Uninstalling the Provisioning Server Component

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

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

1. Select **Management Portal: Provisioning Server**
2. Click the **Remove** option and confirm
3. When prompted, click **Yes** to complete uninstallation and restart the system

Uninstalling the Database Component

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

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

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

Uninstalling All Other Components

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

1. Management Portal: Web Application (Web Server component)
2. Management Portal: Reporting Application Server (Application Server component)
3. Management Portal: Reporting Extensions (Reporting Extensions component)

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

8. GLOSSARY

A

Audit

A diagnostic process instigated to assess system performance.

C

Certificate

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

Certificate Authority

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

Certificate Revocation Lists (CRL)

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

Cipher

A method used to encrypt text.

Cluster

Multiple networked servers, which form the platform across which the Unified Contact Center Management Portal is deployed.

Commissioning

Any action or process required to setup the Unified Contact Center Management Portal platform that is not setup by the Unified Contact Center Management Portal installer or inherent tools.

Configuration

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

Connection

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

Connectors

Connectors consist of:

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

Cookie

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

Comma Separated File (.CSV)

A method of representing a spreadsheet using a text file. The values are separated by commas, and each record is ended by a line break. The column headers are contained in the first record.

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

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 that 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

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.

World Wide Web (WWW)

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

9. INDEX

U

V

W