# Table of Contents

Preface ...........................................................................................................................................................1  
Purpose ..........................................................................................................................................................1  
Audience .......................................................................................................................................................1  
Organization ................................................................................................................................................2  
Related Documentation...............................................................................................................................2  
Product Naming Conventions....................................................................................................................3  
Conventions................................................................................................................................................4  
Obtaining Documentation and Submitting a Service Request.................................................................5  
Documentation Feedback............................................................................................................................5  

1. Administration Overview.............................................................................................................................7  
The Administration & Data Server.............................................................................................................8  
   Unified CCE Tools Folder..........................................................................................................................9  
   Administration Tools Folder...................................................................................................................11  
   Central and Local Databases..................................................................................................................12  
   Lock Administration..............................................................................................................................13  
   How to Acquire and Release a Lock......................................................................................................13  

2. Fault Tolerance..........................................................................................................................................15  
   Architecture..............................................................................................................................................16  
      Approaches to Fault Tolerance..........................................................................................................16  
      Duplicated Communication Paths....................................................................................................17  
      Node Manager....................................................................................................................................18  
   Central Controller...................................................................................................................................18  
      Two Sides............................................................................................................................................19  
      Geographic Distribution....................................................................................................................21  
      Role of the Synchronizers..................................................................................................................22  
      Synchronization and State Transfer.................................................................................................23  
   Database Fault Tolerance.......................................................................................................................25  
      Cisco Unified Intelligent Contact Management Database Recovery...........................................26  
   Network Interface Controllers...............................................................................................................27  
   Peripheral Gateways...............................................................................................................................28  
   Real-Time Administration & Data Servers............................................................................................29  
   Historical Data Servers..........................................................................................................................30  
   Simplexed Operation..............................................................................................................................31  
   Fault Tolerance in Integrated Deployments..........................................................................................31  

3. Working with Databases...........................................................................................................................33  
   Overview..................................................................................................................................................34  
   Types of Data..........................................................................................................................................35  
      Configuration and Script Data...........................................................................................................35  
      Historical and Real-time Data............................................................................................................35  
   Central Database...................................................................................................................................36  
      Database Sizing and Creation............................................................................................................37  
      Database Updates and Changes..........................................................................................................38  
   Local Database (AWDB)..........................................................................................................................38  
      Database Creation and Initialization..................................................................................................38  
      Real-time Data...................................................................................................................................38  
   Configuration Management Service (CMS)............................................................................................39  
   Temporary Database..............................................................................................................................40
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Duplexed Unified ICME Fault Tolerance</td>
<td>17</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Duplexed Central Controller</td>
<td>19</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Central Controller Failure Scenarios</td>
<td>20</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Role of the Synchronizers</td>
<td>22</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Unified ICME Fault-Tolerant Architecture</td>
<td>23</td>
</tr>
<tr>
<td>Figure 6</td>
<td>NIC Fault Tolerance</td>
<td>28</td>
</tr>
<tr>
<td>Figure 7</td>
<td>PG Fault Tolerance</td>
<td>29</td>
</tr>
<tr>
<td>Figure 8</td>
<td>The Unified ICME Databases</td>
<td>34</td>
</tr>
<tr>
<td>Figure 9</td>
<td>CMS Integrated Architecture</td>
<td>39</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Historical Data Server Architecture</td>
<td>40</td>
</tr>
<tr>
<td>Figure 11</td>
<td>Lock Admin Tool</td>
<td>43</td>
</tr>
<tr>
<td>Figure 12</td>
<td>ICMDBA Main Window</td>
<td>48</td>
</tr>
<tr>
<td>Figure 13</td>
<td>Expand Database Window</td>
<td>52</td>
</tr>
<tr>
<td>Figure 14</td>
<td>Synchronize Window</td>
<td>55</td>
</tr>
<tr>
<td>Figure 15</td>
<td>Add Server Window</td>
<td>56</td>
</tr>
<tr>
<td>Figure 16</td>
<td>Configure Window</td>
<td>57</td>
</tr>
<tr>
<td>Figure 17</td>
<td>Database Sizing Estimator</td>
<td>59</td>
</tr>
<tr>
<td>Figure 18</td>
<td>DUMPLOG Example of Per-Process Event Log File</td>
<td>62</td>
</tr>
<tr>
<td>Figure 19</td>
<td>Integrity Check Dialog Box</td>
<td>67</td>
</tr>
<tr>
<td>Figure 20</td>
<td>Synchronize Window</td>
<td>72</td>
</tr>
<tr>
<td>Figure 21</td>
<td>The ICM ID Finder Tool</td>
<td>76</td>
</tr>
<tr>
<td>Figure 22</td>
<td>ICM ID Finder Tool: ID Types</td>
<td>77</td>
</tr>
</tbody>
</table>
Preface

Purpose

This manual describes how to administer and manage Cisco Unified Intelligent Contact Management (Unified ICM) software. It includes information about database administration, event management, support services, and the system software’s fault tolerant architecture.

This manual includes some discussions of how the system software functions in integrated environments with the Cisco Unified E-Mail Interaction Manager (Unified EIM) and Cisco Unified Web Interaction Manager (Unified WIM) components, but it does not provide administration information for the Unified EIM and Unified WIM components. Refer to the appropriate Unified EIM and Unified WIM documentation at http://www.cisco.com/en/US/products/p7236/tsd_products_support_series_home.html and http://www.cisco.com/en/US/products/p7233/tsd_products_support_series_home.html for instructions on how to administer these components.

Audience

This manual is intended for personnel responsible for administering the system software. As a Unified ICM administrator, you should be familiar with Microsoft SQL Server database administration and Windows 2003. This manual also assumes that you have a general understanding of the Unified ICM system components and how they work together as a complete call routing system. Administrators who are responsible for a Unified ICM system that is part of an integrated environment should also have a general understanding of Unified EIM and Unified WIM system components.
Organization

The manual is divided into the following chapters.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, &quot;Administration Overview&quot; (page 7)</td>
<td>Describes aspects of the system that are of interest to the administrator.</td>
</tr>
<tr>
<td>Chapter 2, &quot;Fault Tolerance&quot; (page 15)</td>
<td>Describes the main features of the Unified ICM fault tolerant architecture, with special emphasis on how fault tolerance affects the administration of the system.</td>
</tr>
<tr>
<td>Chapter 3, &quot;Working with Databases&quot; (page 33)</td>
<td>Introduces the Unified ICM databases and explains how they are used.</td>
</tr>
<tr>
<td>Chapter 4, &quot;Database Administration&quot; (page 45)</td>
<td>Describes the ICMDBA tool, the Database Sizing Estimator applet, and the Database Retriever dialog, used for various database administration tasks.</td>
</tr>
<tr>
<td>Chapter 5, &quot;General Administration&quot; (page 65)</td>
<td>Describes the administration that the system software performs automatically. This chapter also includes several optional administration features that you can use.</td>
</tr>
<tr>
<td>Chapter 6, &quot;Partitioning Overview&quot; (page 81)</td>
<td>Discusses the Unified ICM Partitioning feature, which controls what data individuals are allowed to access within a Unified ICM database. <strong>Note:</strong> Partitioning on new installations is no longer supported and is no longer provided as a checkbox option from the Web Setup windows; that is, you cannot create new partitioning on a server. Although the partitioning checkbox has been removed, upgrading to 8.0(1) does not automatically remove partitioning on an existing system.</td>
</tr>
</tbody>
</table>

Related Documentation

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

Related documentation includes the documentation sets for Cisco CTI Object Server (CTI OS), Cisco Agent Desktop (CAD), Cisco Agent Desktop – Browser Edition (CAD-BE), Cisco Unified Contact Center Management Portal, Cisco Unified Customer Voice Portal (CVP), Cisco Unified IP IVR, Cisco Unified Intelligence Center, and Cisco Support Tools. The following list provides more information.

- For documentation for the Cisco Unified Contact Center products mentioned above, go to [http://www.cisco.com/cisco/web/psa/default.html](http://www.cisco.com/cisco/web/psa/default.html), click Voice and Unified Communications, then click Customer Collaboration, and then click Cisco Unified Contact Center Products or Cisco Unified Voice Self-Service Products, then click the product or option you are interested in.
For troubleshooting tips for the Cisco Unified Contact Center Products mentioned above, go to [http://docwiki.cisco.com/wiki/Category:Troubleshooting](http://docwiki.cisco.com/wiki/Category:Troubleshooting), and then click the product or option you are interested in.

Documentation for Cisco Unified Communications Manager is accessible from: [http://www.cisco.com/cisco/web/psa/default.html](http://www.cisco.com/cisco/web/psa/default.html).


The Product Alert tool is accessible from (login required): [http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice](http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice).


---

### Product Naming Conventions

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

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

<table>
<thead>
<tr>
<th>Old Product Name</th>
<th>New Name (long version)</th>
<th>New Name (short version)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IPCC Enterprise Edition</td>
<td>Cisco Unified Contact Center Enterprise</td>
<td>Unified CCE</td>
</tr>
<tr>
<td>Cisco System IPCC Enterprise Edition</td>
<td>Cisco Unified System Contact Center Enterprise</td>
<td>Unified SCCE</td>
</tr>
<tr>
<td><strong>Note:</strong> Cisco Unified System Contact Center Enterprise (Unified SCCE) is supported in 8.0(1); however, there is not a separate 8.0(1) version. If you request features that are in 8.0(1), you must migrate to the Unified ICM/CCE/CCH software. Full migration information is documented in the <em>Upgrade Guide for Cisco Unified ICM/Contact Center Enterprise &amp; Hosted.</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco IPCC Hosted Edition</td>
<td>Cisco Unified Contact Center Hosted</td>
<td>Unified CCH</td>
</tr>
</tbody>
</table>
## Conventions

This manual uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example:</td>
</tr>
<tr>
<td></td>
<td>• Choose <strong>Edit &gt; Find</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Finish</strong>.</td>
</tr>
<tr>
<td><strong>italic</strong> font</td>
<td>Italic font is used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• To introduce a new term; for example: <em>A skill group</em> is a collection of agents who share similar skills.</td>
</tr>
<tr>
<td></td>
<td>• For emphasis; for example: <em>Do not</em> use the numerical naming convention.</td>
</tr>
<tr>
<td></td>
<td>• A syntax value that the user must replace; for example: <em>IF (condition, true-value, false-value)</em></td>
</tr>
<tr>
<td></td>
<td>• A book title; for example: Refer to the <em>Cisco CRS Installation Guide</em></td>
</tr>
<tr>
<td><strong>window font</strong></td>
<td>Window font, such as Courier, is used for the following:</td>
</tr>
<tr>
<td></td>
<td>• Text as it appears in code or that the window displays; for example: <em>&lt;html&gt;&lt;title&gt;Cisco Systems, Inc. &lt;/title&gt;&lt;/html&gt;</em></td>
</tr>
<tr>
<td></td>
<td>• Navigational text when selecting menu options; for example: <em>ICM Configuration Manager &gt; Tools &gt; Explorer Tools &gt; Agent Explorer</em></td>
</tr>
<tr>
<td><strong>&lt; &gt;</strong></td>
<td>Angle brackets are used to indicate the following:</td>
</tr>
</tbody>
</table>
Table:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For arguments where the context does not allow italic, such as ASCII output</td>
</tr>
<tr>
<td></td>
<td>• A character string that the user enters but that does not appear on the window such as a password</td>
</tr>
</tbody>
</table>

Obtaining Documentation and Submitting a Service Request

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:


Subscribe to *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Documentation Feedback

You can provide comments about this document by sending an email message to the following address:

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.
Chapter 1

Administration Overview

This section provides an administration overview of Cisco Unified Intelligent Contact Management (Unified ICM) software (documented as "system software" in this guide).

There are some aspects about administrating the Unified ICM system that you need to understand:

- **Fault Tolerant Architecture.** The fault tolerant architecture of the Unified ICM system ensures continuous operation in the event of hardware or software failures. Certain system administration tasks might not be necessary depending on the level of fault tolerance present in your Unified ICM system. You should review the Unified ICM’s fault tolerant features in order to gain a better understanding of overall system administration.

- **Unified ICM Databases.** The central database resides on the Central Controller and is used for persistent storage of data. In addition, each Administration & Data Server has its own local database (awdb). The local database (awdb) is used for real-time reporting and storing configuration data and scripts. You should understand how these databases are used in the system. You should also become familiar with the tools that manage the data in these databases.

- **Database Storage.** The Unified ICM databases are sized and set up at installation to suit your particular contact center requirements. However, you might want to become familiar with the aspects of system usage that affect database storage capacity. You might also want to review the criteria for sizing the Unified ICM central database.

- **General Administration.** Although most administration is taken care of automatically by the system, there are several optional administration features you should be aware of (especially if configuration uses a simplex Central Controller). These include backing up the central database, performing manual integrity checks on the local database (awdb), and examining the Logger’s event log files.

  **Note:** Simplexing is not supported in a production environment.

- **Running programs from Windows Server 2008 with Service Pack 2 or later systems.** When you run programs from a Windows Server 2008 system with User Account Control
enabled, Windows needs your permission to continue, so click **Allow** in the User Account Control window to run the programs.

- **Event Management.** Familiarize yourself with the Unified ICM’s event management system. The system software provides several tools for reviewing event data in the system. Event data can aid you in identifying potential system performance problems.

- **Partitioning.** Unified ICM partitioning provides a mechanism for controlling what data individuals are allowed to access within an Unified ICM database.

  **Note:**

  - Partitioning on new installations is no longer supported and is no longer provided as a checkbox option from the Web Setup windows; that is, you cannot create new partitioning on a server. Although the partitioning checkbox has been removed, upgrading to 8.0(1) does not automatically remove partitioning on an existing system.

  - See Chapter 6, "Partitioning Overview (page 81)," for support details about upgrading systems that are already partitioned.

The following chapters describe these topics in more detail.

**The Administration & Data Server**

The Administration & Data Server provides tools and resources for supervisors, system administrators, and system managers.

You can use these resources to:

- Initialize and update configuration information
- Write and update routing scripts and administrative scripts
- Monitor the execution of scripts

You can also monitor the performance of skill groups, services, routes, and trunks through the Administration & Data Server.

The installation process installs the **Unified CCE Tools (page 9)** folder on the desktop, and provides the **Cisco Unified CCE Tools** menu option on the Start menu (**Start > All Programs > Cisco Unified CCE Tools**).

**Note:** The Administration Tools are only included in this folder if an Administration & Data Server is set up on the machine.

After you add an Administration & Data Server, the following happens:
Chapter 1: Administration Overview

The Unified CCE Administration Tools (page 11) folder displays on the desktop, along with the Administration Tools menu option on the Start menu (Start > All Programs > Cisco Unified CCE Tools > Administration Tools).

The Administration Tools icon displays in the Unified CCE Tools folder, which is a shortcut to the Administration Tools folder.

Unified CCE Tools Folder

Users with Setup rights and who are part of a Local Admin group can run the following tools:

- ICMdba
- Peripheral Gateway Setup
- Service Control
- SSL Encryption Utility
- Service Account Manager
- Administration Client Setup
- Web Setup
- Unified System CLI Tool

The following tools are available in this folder:

- **Administration Client Setup.** Sets up Administration Client(s) for ICM/CCE/CCH Instance(s) on a machine. An Administration Client is a lightweight remote administration interface to an Administration & Data Server. An Instance is a single logical Unified ICM/CCE/CCH.

- **Domain Manager.** Allows the creation of Organizational Units (OU) along with groups and permissions associated with each OU. It also allows you to give user permissions to various Unified ICM tasks.

- **Glossary.** Defines terms related to the system software.

- **ICMdba.** Provides a central utility that allows you to create new databases, modify or delete existing databases, and perform limited SQL Server configuration tasks.

- **Performance Monitor** (For Windows 2008 R2 systems only). This shortcut launches the 32-bit version of perfmon so that Unified CCE 32-bit process can easily be monitored.

- **Peripheral Gateway Setup** (PG Setup). A Unified ICM/CCE/CCH tool with which administrators and system administrators can set up Peripheral Gateways (PGs) and their associated Peripheral Interface Managers (PIMs), CTI Server, Outbound Option Dialer, and CompuCALL Server Gateway.
• **Security Wizard.** A security deployment tool for Unified ICM/CCE, which can be used to harden the system security, configure Windows firewall, or apply pre-defined IPSec policies for the Contact Center application. This wizard provides a graphical user interface to execute Unified ICM/CCE command-line security utilities and simplifies security configuration through its step-by-step wizard based approach.

**Note:** For more information, refer to *Security Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 8.x(y).*

• **Service Control.** Lets you stop and start Unified ICM-related services.

**Note:** Service Control is not available on Administration Client systems.

• **SSL Encryption Utility.** Enables changing the default SSL settings (implemented by the Cisco Unified ICM/Contact Center Enterprise & Hosted Installer) and further configure WebView to enable encryption for the entire session, as opposed to only user authentication. The SSL Encryption Utility contains the functionality to re-generate the self-signed certificate and replace the IIS installed certificate, as needed.

• **Administration Tools.** Provides shortcut to the Administration Tools (page 11) folder.

• **Service Account Manager (SAM).** Allows you to manipulate the default service account creation process.

This provides you with the needed flexibility to:

– Either create a new service account or select one created prior to setup.

– Enter your own password or let the Unified ICM application generate one for you.

**Note:** If passwords are changed using an application other than SAM, SAM cannot detect the changes.

– To choose (when applicable) whether or not to update the account in Active Directory (AD) and use existing AD accounts as Unified ICM service accounts.

– Fix service account group membership issues (such as modifying Unified ICM service account passwords) without recreating accounts or without re-running setup.

• **Unified System CLI Tool.** A command line interface that retrieves diagnostic data (supports the REST-like RPC-Hybrid interface).

• **Web Setup.** A browser-based application with which Unified ICM/CCE/CCH administrators and system administrators can manage instances, add and modify Unified ICM/CCE/CCH components, and manage Unified ICM/CCE/CCH-related system services.

For Windows 2008 R2, the following applications can only be invoked by users who are members of an instance Setup group, and local Admin group members (which is the default behavior on Windows 2008 R2). Upon invocation, each application will display the User Account Control (UAC) dialog with the publisher displayed as “Cisco UCCE”. Afterwards, the user may either run the application or shut it down. If the publisher is displayed as anything other than “Cisco UCCE”, the user **must not** continue to run the application since it may be compromised. If a
non-Setup/Administrators user tries to invoke these applications, the UAC dialog will ask for the credentials of a Setup/Administrators user before allowing the application invocation.

- cmscontrol.exe
- ICMDBA.exe
- ServiceControl.exe
- SSLUtil.exe
- ServiceAccountManager.exe
- RegUtil.exe
-instsrv.exe
- conicrSimpleApp.exe
-regacc.exe
-regcmd.exe
-stopshut.exe
-upcctest.exe

The Configuration Manager application (Launcher.exe) allows for instance level Config users to invoke it. However, the active directory tools (User List Tool and Agent Explorer Tool) within Configuration Manager will fail if they try to access Active Directory. For all the tools to function properly, the Config user can right-click on the icon and click on “Run as Administrator”, and then provide the credentials of a Setup user. If the logon user is a Setup user, the Configuration Manager will work properly for all the tools in it.

See Also

Refer to the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for detailed information about the installation process.

Administration Tools Folder

The following tools are available in this folder:

- **Call Tracer.** Lets you send test calls to the system software and see how they are processed and the target chosen.

- **Check Routes.** Lets you validate the configuration of routes referenced by a script.

- **Configuration Manager.** Lets you set up and maintain your environment. The configuration includes the hardware within the system, the services provided by the system, and the agents who provide them.
• **Initialize Local Database.** Lets you copy current information from the system software’s central database to the local database (awdb) on the Administration & Data Server. (Normally, this is done automatically.)

• **Lock Admin.** Lets you check or change the status of locks in the system software central database.

• **Router Log Viewer.** Displays information about calls processed by the system software and any errors encountered in processing them.

• **Scheduled Target Manager.** Lets you configure and manage scheduled targets, which indicate a special type of destination for a call.

• **Schema Help.** Describes the structure of the Unified ICM databases.

• **Script Editor.** Lets you create, modify, and schedule routing scripts. The system software executes these scripts to determine where to route each call.

• **Select Administration Instance.** Allows you to switch between administration instances.

• **CMS Control Tool.** The Configuration Management Service (CMS) Control console is the control panel for CMS Node. CMS allows the Agent Re-skilling Web Tool and the CMS Node options access to the configuration.

  **Note:** This tool only displays if the Configuration Management Service (CMS) Node is enabled in the Administration & Data Server.

**Note:** The availability of some of these tools depends on the Administration & Data Server's role. (See the "Historical Data Server (page ?)" section for an explanation of the roles).

**See Also**

Refer to the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for detailed information about the installation process.

**Central and Local Databases**

The Central Controller includes a database that stores the system configuration information and routing scripts. At least one Administration & Data Server at each site has its own local database that contains a copy of data from the central database. Unified ICM software’s UpdateAW background process automatically keeps the local database synchronized with the central database.

An Administration Client, which does not have a local database, points to a local database (awdb) for its data.

When you save a change to configuration data or scripts, the system software immediately applies that change to the central database. The UpdateAW process copies the change to all local databases.
Lock Administration

To modify a script, you must first obtain a lock on that script. This prevents other users from changing the same script until you have saved your changes. When you edit a script, the Script Editor automatically acquires a script lock for you. The script lock applies to only one script.

Optionally, you can obtain a master lock that prevents other users from making any changes to scripts or configuration data. The master lock is for backwards compatibility only. If a user holds the master lock, only that user can make changes to any scripts or configuration data.

How to Acquire and Release a Lock

To acquire and release a lock, follow these steps:

Step 1  Start Lock Admin from the Administration & Data Server group or the Administration Client group. The Lock Admin dialog box appears, showing the status of all locks.

Step 2  Select the lock by clicking on the Type column of the row describing the lock.

Step 3  Select Release.

Step 4  Select Close when done.

See Also

For information on registering users and setting up security for the Unified ICM system, refer to the Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted and the Security Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 8.x(y). The installation guide also contains information on networking requirements and configuration options for the Unified ICM system components.
Chapter 2

Fault Tolerance

The system software is a fault tolerant call routing system that continues to operate without interruption in the case of hardware, software, or communications failures. The main goals of Unified ICM’s fault tolerant architecture are to:

- Minimize time periods during which the system is non-responsive to call routing requests (for example, while the system is being reconfigured due to a component failure or recovery).
- Eliminate all single points of failure that would cause the system to stop.
- Provide disaster protection by allowing the major system components to be geographically separated.

Unified ICM’s fault tolerant mechanisms operate in the background and are not visible from within Unified ICM applications. However, it is still important that you have a general understanding of the fault tolerant architecture and the implications it has for system administration.

In some cases, the level of fault tolerance in the Unified ICM system can affect which administration tasks you need to perform. For example, in duplexed database configurations many typical database administration tasks such as database backups become unnecessary because exact copies of the central database are kept on each side of the system on separate computers.

This chapter provides an overview of Unified ICM fault tolerance with a special emphasis on the fault tolerance of the Central Controller and the central database.

This chapter contains the following topics:

- Architecture, page 16
- Central Controller, page 18
- Database Fault Tolerance, page 25
- Network Interface Controllers, page 27
The architecture of the system software allows the system to continue to function if one component fails. This ability is called fault tolerance. To ensure that the system software continues to operate in the case of a computer failure, all critical parts of the system can be physically duplicated. There can be two or more physical Network Interface Controllers (NICs), two physical Peripheral Gateways (PGs) at each call center, and two Central Controllers. The communication paths between critical components can also be duplicated.

The critical components of the system software include the Central Controller (CallRouter and Logger), PGs, and NICs. Normal non-HDS Administration & Data Servers and Administration Clients are not considered to be critical to the operation of the system since they play no active role in routing calls or storing historical data.

When both sides of a component (that is, Side A and Side B) are available to the system, that component is said to be duplexed; when only one of the pair is available, the component is running by itself, if it is set up as duplexed. You might have some components in your Unified ICM system that are duplexed and others that are simplexed. For example, you might have a duplexed Central Controller (two CallRouters and two Loggers) and simplexed Peripheral Gateways (in lab environment only) at call center sites.

It takes more than duplicate hardware to achieve fault tolerance. The Unified ICM system can quickly detect that a component has failed, bypass that component, and use its duplicate instead. The system software can also initiate diagnostics and service so that the failed component can be fixed or replaced and the system returned to duplexed operation.

Approaches to Fault Tolerance

The system software uses two approaches to fault tolerance: hot standby and synchronized execution. In the hot standby approach, one set of processes is called the primary, and the other is called the backup. In this model, the primary process performs the work at hand while the backup process is idle. In the event of a primary process failure, the backup process is activated and takes over. Peripheral Gateways optionally use the hot standby approach to fault tolerance.

The system software uses synchronized execution in the Central Controller. In the synchronized execution approach, all critical processes (CallRouter and Logger) are duplicated on separate computers. There is no concept of primary or backup. Both process sets run in a synchronized fashion, processing duplicate input and producing duplicate output. Each synchronized system is an equal peer. Each set of peers is a synchronized process pair.

In the event that one of the synchronized processes fails (for example, a CallRouter goes off-line), its peer continues to run. There is no loss of data and calls continue to be routed. When the failed member of the pair returns to operation, it is resynchronized with its peer and begins to
run again as a synchronized process. The following figure shows how synchronized execution and hot standby are applied in the system software.

**Figure 1: Duplexed Unified ICME Fault Tolerance**

PGs and NICs use the hot standby approach to fault tolerance. Note that the duplexed NIC in the figure above is implemented on two separate computers. Each computer has active and idle connections to the sides of the Central Controller. NIC fault tolerance is described in more detail later in this chapter.

**Duplicated Communication Paths**

Each NIC, Peripheral Gateway, and Administration & Data Server or Administration Client has two communication paths to the Central Controller (see above figure). The two paths connect the device (for example, a PG) to a Central Controller Agent process on each side of the Central Controller. The Central Controller Agent is a software process that manages communications between the Central Controller and nodes in the Unified ICM system.

At any one time, one of the two communications paths is active and the other is idle. All communication traffic between the Central Controller and the device is sent on the active path. If the active path fails for any reason, the second path is activated and all traffic is switched to the newly active path. The previously active path becomes the idle path.

The communication protocols use buffering and acknowledgments to ensure that no messages are lost during the path failure and switch-over. After a communication path failure, the device periodically attempts to re-establish communication along the failed path.
A different mechanism is used for the real-time data feed to Administration & Data Servers or Administration Clients. See the "Real-Time Administration & Data Servers (page 30)" section, for more information.

Node Manager

Each Unified ICM component (except the Administration Client) includes a Node Manager process. The Node Manager is in charge of restarting Intelligent Contact Management processes that have failed. For example, each Logger and each CallRouter has its own Node Manager. If a Logger and CallRouter are installed on the same machine, two separate Node Managers run on that machine. If Loggers for multiple customers run on a single machine, a separate Node Manager runs for each customer.

When a failure occurs in a single-customer Unified ICM system, the Node Manager might shut down the machine to initiate a reboot. However, in a Cisco Unified Intelligent Contact Management Hosted environment when a Logger or CallRouter fails, components for other customers might still be active on the machine. In such a case, the Node Manager for a Cisco Unified Intelligent Contact Management Hosted component does not shut down and reboot the machine, and manual intervention is required to restore the failed component.

If the Node Manager does initiate a reboot, the Node Manager itself restarts when the machine reboots. The Node Manager then starts the other processes for the component.

To set up automatic restart for any component, access the Web Setup tool's Service Management page to set a component's service as Automatic rather than Manual.

See Also

For more information on Node Manager start-up options, refer to the Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted.

Central Controller

The Central Controller includes the CallRouter and Logger. The CallRouter and Logger processes are typically on separate computers. However, in smaller call center configurations the CallRouter and Logger processes can be on the same computer. The Logger process is always on the same computer.

Note: Beginning with Unified ICM 7.0(0), the Logger changed from a single process to two running processes—one process handling configuration data and the other handling historical data. This allows parallel processing of the two kinds of data and, thus, a more efficient Logger. However, these two processes are still part of a single Logger node; that is, the functionality of the Logger remains essentially unchanged. Therefore, throughout this manual, reference will generally continue to be made to the Logger, without distinguishing between the separate processes. However, you should be aware that the new split in the Logger does affect failure and failover behavior. For example, if the historical Logger on side A fails, the system fails over to the historical Logger on side B; however, the still functioning configuration Logger on side A continues to be used.
A duplexed Central Controller uses the synchronized execution approach to fault tolerance. The Central Controller processes are duplicated and run as synchronized process pairs. In synchronized execution, if one component fails its peer continues running and the system runs without interruption. The Database Manager is also duplicated, but technically it does not run synchronized. Since all modifications to the database come through the Logger, the databases automatically remain synchronized.

Two Sides

All components of the Central Controller, with their duplicates, form one logical duplexed system. The system can be divided into two sides, each of which contains one side of a component. Each side of the Central Controller has a Database Manager, Logger, CallRouter, Synchronizer, and an Agent. By convention, the two sides are referred to as Side A and Side B.

All components, processes, and configuration objects within a side are collocated; that is, located on the same local area network (LAN). However, Side A might be geographically separated from Side B. The following figure shows the two sides of a duplexed Central Controller.

During normal operation, the two sides run in parallel. For example, information about each incoming call is processed by both CallRouters. Both CallRouters, using the same call routing scripts and identical information about the call centers, determine the same destination for the call. Both sides of the Central Controller receive the same information from the Peripheral Gateways and Administration & Data Servers or Administration Clients.

A duplexed Central Controller can tolerate a single device or system failure (for example, the loss of one CallRouter) without losing functions. A double failure, while extremely rare, typically results in some loss of functions. An example of a double failure would be if both CallRouters in a duplexed system were to go off-line.
Single failures are typically caused by system crashes, operating system failures, or disk failures. However, LAN outages and IP router failures can also cause single failures. The following figure shows five possible Central Controller failure scenarios.

Each of these failures affects system functions differently:

- **Single Logger.** If a single Logger (whether historical or configuration Logger) goes off-line, the system software runs without interruption. All call routing and reporting functions remain available. The CallRouters continue to operate as a synchronized pair. The remaining Logger runs simplex. When the failed Logger returns to service, the Loggers return to synchronized execution.
• **Single CallRouter.** When a CallRouter on one side of the Central Controller fails, that entire side of the Central Controller is removed from service. This is because the CallRouter plays an integral part in forwarding historical data to the historical Logger on its side of the system. The on-line side of the Central Controller runs as a simplex system. Call processing continues uninterrupted and reporting functions are still available. When the failed CallRouter returns to service, both CallRouters and both Loggers return to synchronized execution.

• **Logger and CallRouter (opposite sides).** In this failure scenario, side B of the Central Controller is removed from service due to the CallRouter failure. Call routing continues uninterrupted with the remaining Side A CallRouter; however, data in both databases slowly becomes out of date. Some reporting functions are not available until the nodes are returned to service and synchronized execution is restored.

• **Both Loggers.** In a double Logger failure, call routing continues uninterrupted. If it is the historical Loggers that failed, all reporting functions are lost until at least one of the historical Loggers returns. If it is the configuration Loggers that failed, you cannot make any configuration changes until at least one configuration Logger is operational. Such a double failure is extremely rare. The CallRouter continues to route calls because it has a copy of the call center enterprise configuration data in its program memory. (The CallRouter loads the configuration data into memory when it is started and keeps it up-to-date as configuration changes occur.)

• **One Side.** If one side of the Central Controller goes off-line, processing continues uninterrupted. The system software continues to function as a simplex system until the failed side of the Central Controller returns to service. All functions remain, but the system is running simplex (without protection against an additional failure). When the off-line side of the Central Controller returns, normal duplexed operation is restored.

A double CallRouter failure would temporarily disrupt call routing and reporting functions. This type of failure is extremely rare (especially in geographically distributed Central Controller configurations).

**Geographic Distribution**

To provide maximum protection against disasters such as fires, floods, and earthquakes, the two sides of the Central Controller can be in separate locations—even in separate cities. The two Synchronizers communicate with each other via a private wide area network (WAN) to ensure that they remain synchronized. This WAN, called the private WAN, is used for no other purpose than to ensure synchronization between the sides of the Central Controller.

**See Also**

For details on collocated and distributed Central Controller configurations, refer to the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted.*
Role of the Synchronizers

The Synchronizers play the key role in maintaining synchronized execution across the two sides of the Central Controller. All input for the CallRouter and any changes to the Logger must pass through the Synchronizers.

Each time a Synchronizer receives input, it passes that input to its duplicate on the other side. The two Synchronizers cooperate to ensure that they are both sending the same input to the Central Controllers on both sides of the system.

The following figure shows how the Synchronizers combine input messages and send the messages in the same order to each side of the Central Controller.

Figure 4: Role of the Synchronizers

Both CallRouters receive the same input and generate the same output. The Synchronizers ensure that both sides of the Central Controller return identical destinations for the same call and write identical data to the databases.

The following figure further illustrates the Central Controller and its device connections.
Each PG, NIC, and Administration & Data Server or Administration Client has duplicate communication paths to the Central Controller. If there is a failure on one side of the Central Controller, the PGs, NICs, and Administration & Data Servers or Administration Clients can switch their communication paths to the active side of the Central Controller. As shown in the above figure, only one communication path is active at a time. The other communication path is idle (indicated by a dotted line). The system software sends heartbeats (brief periodic messages) over the idle path to ensure that it can still be used in the event that the active path fails.

**Synchronization and State Transfer**

In synchronized execution, duplicated processes are always processing identical input and generating identical output. If one process fails, the other continues to operate without interrupting
system operation. Once the failed process returns, it is immediately updated with the current state of Unified ICM processes running on its peer.

In order to synchronize one peer with another after a failure, the system performs a state transfer. The state transfer facility allows a synchronized process (for example, a CallRouter) to copy the variables in its memory to its peer. The recovering system receives the variables from the currently executing system and is able to restart with a copy of the current state of Unified ICM processes. For example, as soon as a failure is detected on the Side A CallRouter, the system software only uses Side B. When the Side A CallRouter is restarted, the system software invokes a state transfer to immediately update the Central Controller Side A components with the current state of their counterparts on Side B.

In order to better understand synchronization and state transfer, it might help to take a closer look at CallRouter and Logger recovery.

CallRouter Recovery

When a single CallRouter process fails for any reason, the system software continues to operate without any loss of functions by using the other side of the Central Controller. All attached devices (PGs, NICs, and Administration & Data Servers or Administration Clients) switch their active communications paths to the remaining side. This ensures that devices such as PGs continue to receive CallRouter output through the active CallRouter on the other side of the system.

As a consequence of the CallRouter failure, the entire side of the Central Controller is removed from service. The Logger associated with the failed CallRouter sees no further inputs (and will not until the failed CallRouter is restored to full operation). All components on the failed side of the Central Controller lose synchronization with the other side. The CallRouter and Logger must all be resynchronized before normal duplexed operation can resume.

For a single-instance Unified ICM, the recovery process begins when the Node Manager notices the failure of a CallRouter process and automatically restarts it. Other processes are not impacted. In a Cisco Unified Intelligent Contact Management Hosted environment, if several Unified ICM instances are running on the same machine, the Node Manager cannot restart the machine. In such Cisco Unified Intelligent Contact Management Hosted environments, manual intervention is required to restart the failed CallRouter process.

The restarted CallRouter immediately initiates a state transfer from its currently executing peer. Each CallRouter sends a message to its Logger. The Loggers then perform their own state transfer.

When the state transfer is completed, all processes are now synchronized. The newly on-line Central Controller sends an in-service status to all local Agents. It then begins processing input messages. After the state transfer, both sides of the Central Controller see exactly the same sequence of input messages. At this point the Unified ICM system is returned to full duplexed operation.
Logger Recovery

When a single Logger process fails, the system software continues to operate with the Logger on the other side. The remaining Logger ensures that output messages continue to reach PGs and Administration & Data Servers. The Unified ICM’s Message Delivery Service detects the failure of the Logger and notifies the PGs and Administration & Data Servers, which switch their active communication paths to the on-line Logger. At this point, both CallRouters are in service, but only one Logger is available.

For a single-customer Unified ICM, when the Node Manager detects that the Logger has gone off-line, it initiates a shutdown and reboot of the machine. In a Cisco Unified Intelligent Contact Management Hosted environment, the Node Manager does not restart the machine. In this case, manual intervention is needed to restart the failed Logger.

The Logger’s Node Manager automatically restarts when the machine reboots. Next, the SQL Server service starts automatically as part of the reboot. SQL Server automatic recovery runs to ensure that the returning database is consistent and that all transactions committed before the failure are recorded on disk. Once automatic recovery is completed, the Logger can then go through the application synchronization and state transfer process. If configuration data in the on-line database has changed, the state transfer also updates the configuration data in the returning database. However, in most cases configuration data will not have changed during the failure.

Once the two Loggers are returned to synchronized execution, the system software might need to recover historical data that was accumulated during the off-line period. This process, referred to as Recovery, is described in the "Database Fault Tolerance" section.

In a double Logger failure (both Loggers are off-line), the CallRouter continues to route calls. This is possible, even if it is the configuration Loggers that have failed, because the CallRouter loads configuration data in its program memory at system initialization. In a double Logger failure scenario, all messages and data that the CallRouter sends to an off-line Logger are discarded until a Logger is completely recovered.

Database Fault Tolerance

The Central Controller database provides two major Unified ICM functions:

- Permanent storage of the data that describes a call routing configuration.
- Permanent storage for the historical data that is gathered by the Unified ICM system.

Each time a CallRouter starts, it loads configuration data from the central database into its program memory. Once the configuration data is loaded, the CallRouter can begin to route calls (even when the central database is not available). Therefore, when a CallRouter fails and restarts, at least one configuration Logger and central database must be available so that the CallRouter can load the configuration data into memory.
In addition to configuration data, Peripheral Gateways, NICs, and the CallRouter itself all produce historical data. The system components gather historical data and pass it to the CallRouter, which then delivers it to the historical Logger and the central database. The historical Logger passes the historical data on to an Historical Data Server (HDS) facility on an Administration & Data Server.

The ability of the CallRouter to deliver data to the historical Logger and the central database is not necessary for call routing. However, Unified ICM’s monitoring and reporting facilities require both real-time data and historical data from the central database. Database fault tolerance and data recovery, therefore, are extremely important to the reporting functions of Unified ICM software.

Cisco Unified Intelligent Contact Management Database Recovery

Database recovery is the process of bringing an off-line database up to the same state as an on-line database. In a database device failure (for example, in a disk failure), some manual intervention is required to restore duplexed operation and bring the off-line database up to date. The following scenarios describe what happens in a system failure, a disk failure, and a software failure.

System Failure

When a single Logger, CallRouter, or Database Manager fails (for example, due to a power outage), the associated central database will go off-line. The process of bringing the off-line database back to full synchronization is completely automatic. If the Logger machine reboots, SQL Server automatic recovery runs to ensure that the database is consistent and that all transactions committed before the failure are recorded on disk.

**Note:** If the Logger machine does not reboot, SQL Server automatic recovery is not required.

After SQL Server automatic recovery is completed, the off-line Logger synchronizes its state with the state of the on-line Logger. After the state transfer process takes place, both members of the Logger pair can execute as a synchronized process pair.

During the time that one database is off-line, configuration data might have been added to the contents of the on-line database. If any configuration data changed while one database was off-line, the configuration changes are applied to the database as part of the configuration Logger’s state transfer process. This configuration update happens as part of the state transfer before synchronized execution begins.

Any historical data that accumulated in the on-line database is recovered after synchronized execution begins. Rather than attempting to recover the historical data immediately, the system software first restores system fault tolerance (that is, duplexed database capability and synchronized execution).

The system software recovers historical data from the on-line database using a special process called Recovery. In Recovery, the historical Logger communicates with its counterpart on the other side of the Central Controller and requests any historical data that was inserted during the off-line period. The counterpart delivers the data over the private network that connects both sides of a duplexed Central Controller.
Disk Failure

A disk failure requires additional steps. If a disk failure disables one side of the Central Controller database, the disk must be repaired or replaced.

**Note:** Contact your Unified ICM support provider if a disk failure occurs.

---

**Step 1**
Rebuild the database structure from scratch on the new disks.

**Step 2**
Restore the configuration data, either from:

- A snapshot of the on-line database.
- The most recent backup tape.
- A backup tape taken from the on-line side of the Central Controller database.
- ICMDBA tool using a synchronization operation with the other side of the Logger.

At the time of the state transfer, any missing configuration data will be restored. Historical data is restored by the Recovery process, which is run automatically each time the Node Manager process starts on the Logger, or by loading the data from a backup tape.

Software Failure

Cases of software failure that leave a Central Controller database unavailable are handled in the same way as a disk failure (if the failure cannot be repaired by existing software tools). Contact your Unified ICM support provider if such a failure occurs.

Network Interface Controllers

The NIC has four physical controllers on each side of the Central Controller. Each of these controllers can simultaneously handle calls from the signaling network. Typically, each physical NIC handles part of the total call routing load for the system software.

The NIC processes are implemented as non-synchronized process pairs (one process on each side of the Central Controller). The NIC runs as a process on the CallRouter machine.

As a non-synchronized process pair, the NICs operate without knowledge of each other. They are managed by the Node Manager and communicate with other CallRouter processes via the Message Delivery Service (MDS). The following figure shows how fault tolerance is implemented for various NICs.
Figure 6: NIC Fault Tolerance

In a duplexed environment, two NICs are on-line and handling routing requests simultaneously. Typically, each NIC handles part of the total call routing load for the system software. The Synchronizers combine the two input streams to ensure that both sides of the Central Controller receive the same routing requests. If one of the NIC processes fails, or one side of the Central Controller is removed from service, the signaling network detects that communication is no longer possible to that NIC and automatically sends all routing requests to the remaining NIC process.

Peripheral Gateways

Peripheral Gateways use a combination of the synchronization and hot standby approaches to fault tolerance. The Open Peripheral Controller (OPC) operates as a synchronized process pair on a duplexed PG system. The Peripheral Interface Managers (PIMs) typically use the hot standby approach. The following figure shows how synchronization and hot standby are employed in a duplexed Peripheral Gateway (PG).
The OPC processes communicate with each other via a private network connection and the Message Delivery Service (MDS). The MDS provides a synchronizer service which combines the input streams from the PIMs and PG Agents on both sides of the PG to ensure that both OPC processes see exactly the same input.

The OPC process is responsible for activating PIMs and PG Agents on each side of the duplexed PG. The OPC process also supplies uniform message sets from various PG types to the Central Controller.

In Unified ICM, as a default, OPC does not keep calls in memory waiting to be re-initialized upon PIM activation after a PG failover. This might result in calls having calltype, call variables and ECC variables lost on Agent Desktops when a PG failover occurs.

The PIMs manage the interface between different types of ACDs and the OPC. PIMs are duplicated on each side of the system and operate in hot standby mode. A PIM can be active on either side of the duplexed PG, but not on both sides at the same time. For example, in the figure above PIMs 1 and 2 are active on Side A; PIM 3 is active on Side B. The duplexed OPCs communicate with each other through the MDS to ensure that a PIM is active only on one side at a time.

The duplexed PG architecture protects against a failure on one side of the PG. For example, if an adapter card controlling access to an ACD fails, a hot standby PIM can use the alternate PIM activation path. As shown in the above figure, PIM3 has been activated from Side B of the PG. This might be in response to an adapter failure between the Side A PIM3 and ACD3. In this type of failure scenario, the PG is able to maintain communication with the attached ACD.

Only one PG Agent actively communicates with a side of the Central Controller. When messages arrive at the Central Controller, they are delivered to both sides by the Central Controller.
Synchronizer process. The PG maintains idle communication paths to both sides of the Central Controller in case a switch-over to the other side of the Central Controller or PG is necessary.

Real-Time Administration & Data Servers

To allow users to monitor current call center activity, the system software must send up-to-date data to the Administration & Data Server in a reliable and timely manner. The real-time data arrives at the Central Controller from the Peripheral Gateways, which are monitoring activity at each call center. The CallRouter acts as the real-time server. The CallRouter for the other side of the Central Controller is the back-up real-time server.

Administration & Data Servers or Administration Clients can be located with one or both sides of the Central Controller, at a call center, or at another site. Any site that contains Administration & Data Servers is referred to as an admin site.

The CallRouter is responsible for providing real-time data to an Administration & Data Server at each admin site. Each site has at least one, and usually two, Administration & Data Servers that serve as real-time data Administration & Data Servers for the site. The primary Administration & Data Server maintains an active connection to the real-time server through which it receives real-time data.

Administration Clients at the site receive their real-time data through a connection to an Administration & Data Server. Administration Clients do not have the local database and Administration & Data Server processes required to receive real-time data directly from the Central Controller real-time server.

If the site has two Administration & Data Servers, Administration Clients are configured to automatically switch to a secondary Administration & Data Server if the first Administration & Data Server becomes non-functional for any reason. The secondary Administration & Data Server also maintains connections to the real-time server; however, these connections remain idle until needed.

You deploy an Administration & Data Server by installing the software using the Cisco Unified ICM/Contact Center Enterprise & Hosted Installer, and then set up the Administration & Data Server using the Web Setup tool.

You deploy an Administration Client by installing the software using the Administration Client Installer, and then set it up using the Administration Client Setup tool.

See Also

Refer to the Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted for details about installing and setting up the Administration & Data Servers.

Historical Data Servers

Historical data is forwarded to the Administration & Data Server where they are stored in a special database. The server then acts as an Historical Data Server (HDS) for the admin site.
WebView and Cisco Unified Intelligence Center (the reporting tools) at the site query historical data from the HDS rather than directly from the Logger.

Typically, two Administration & Data Servers at a site are set up as primary and secondary servers to support fault tolerance. The HDS must be configured only on the primary Administration & Data Server. If the primary Administration & Data Server fails, the secondary Administration & Data Servers at the site automatically becomes active. (The HDS on the primary server is still active when this occurs.)

See Also

The "Historical Data Server (page ?)" section in Chapter 3, "Working with Databases," provides more information on setting up an HDS Administration & Data Server.

Simplex Operation

If you have a simplexed Central Controller configuration, you are vulnerable to a single device failure (for example, a system failure, process failure, or a disk crash). Have a strategy in place for keeping daily backups of the central database. Your backup strategy might involve regularly scheduled backups, mirrored disk configurations, or Redundant Array of Inexpensive Disk (RAID) configurations. Always have the central database backed up on removable media.

Note: Simplexing is not supported in a production environment.

If the central database becomes unavailable due to disk failure, contact your Unified ICM support provider. A support representative can assist you in replacing the disk, rebuilding the database, and restoring the configuration and historical data.

See Also

For more information on database backup and restore procedures for simplexed Central Controllers, see Chapter 5, "General Administration (page 65)."

Fault Tolerance in Integrated Deployments

Some components in Unified ICM implement synchronized fault-tolerance, meaning that communication paths to redundant components are utilized simultaneously. This reduces the probability of message loss during transition periods to a very low rate. Cisco Media Blender (MB) nodes do not implement synchronized fault-tolerance; however, duplexed implementations of these nodes provides a vast improvement over a single path setup. The Unified WIM and Unified EIM documentation describes general recovery behavior and its effects when a single node failure occurs in an integrated deployment. Although multiple failures are not considered, an instance of multiple node failure will manifest itself as a superposition of single failure cases. However, a catastrophic failure can occur if all redundant components in an array fail (for example, if all routing servers fail).

Note: For detailed information about Unified WIM and Unified EIM fault tolerance, refer to the Cisco Unified Web and E-Mail Interaction Manager, Solution Network Reference Design
Fault Tolerance in Integrated Deployments

The system software stores configuration information and call routing scripts in a central database that is part of the Central Controller. You cannot directly alter data in the central database. Instead, you work with a copy of the configuration and script data that resides in the local database (awdb). When you make changes to these data (for example, by using the Configuration Manager or Script Editor tools), the changes are applied to the local database (awdb) and automatically to the central database on the Logger.

In addition to safeguarding the integrity of data in the central database, the local database (awdb) stores real-time performance statistics. For example, it stores data such as the current Average Delay in Queue, Longest Call in Queue, and the number of Available Agents for each service. This information is updated approximately every ten seconds.

The system software stores historical performance data in the central database and in a special Historical Data Server (HDS) database on the Administration & Data Server.

The following explains where data is stored:

- Real-time data is only stored in the local database (awdb) on the Administration & Data Server when the Administration & Data Server has a Real-time Server role.

- Historical data is only stored in the HDS database on the Administration & Data Server when the Administration & Data Server has an HDS role.

This chapter provides an overview of the Unified ICM databases. In particular, it focuses on the types of data contained in each database and how these data are kept current.

This chapter contains the following topics:

- Overview, page 34
- Types of Data, page 35
- Central Database, page 36
- Local Database (AWDB), page 38
Overview

The following figure shows the Unified ICM databases and how changes made to the Administration & Data Server local data are automatically applied to the central database.

*Figure 8: The Unified ICME Databases*

The *Initialize Local Database tool* copies data from the central database to the local database (awdb). This tool is used to update the local database (awdb). Optionally, you can use this tool to update the local database (awdb) at any time.

**Note:** Until the Initialize Local Database tool operation is completed, configuration changes cannot be made.

Subsequently, the *UpdateAW process* forwards to the local database (awdb) any changes made to the central database. Changes made to configuration data and scripts are automatically copied from the central database back to the local database (awdb).

To make access to the real-time data as efficient as possible, the data are stored in memory in temporary tables. These temporary tables actually reside in the TEMPDB database; however, you can access them as if they were tables within the local database (awdb).

An Administration & Data Server that serves as an Historical Database Server (HDS) has a special database to store historical data it receives from the central database. Administration Clients can then access historical data from the HDS rather than from the central database.
See the "Historical Data Server (page ?)" section for more information on the HDS option.

In a Cisco Unified Intelligent Contact Management Hosted environment, a single machine might serve multiple customers. In this case, each customer has its own database. For example, if a Logger machine runs separate instances for each of 10 customers, then it contains 10 central databases. If an Administration & Data Server needs access to those 10 customers, it needs 10 local databases (awdb).

Regardless of the number of databases, only one instance of SQL Server runs on each machine. One set of SQL Server processes maintain all the databases on the machine.

The Cisco Network Applications Manager Product Description and the Cisco Network Applications Manager User Guide provide more information on multiple customer environments.

Types of Data

The system software handles three types of data:

- **Configuration data** is stored in the central, HDS, and local databases (awdb).
- **Historical data** is stored in the central database and the HDS database.
- **Real-time data** is stored in the local database (awdb).

Configuration and Script Data

*Configuration data* describe your call center enterprise. For example, all of your peripherals, services, dialed numbers, routes, and peripheral targets are part of the configuration data. Configuration data can also include data that has been imported from other systems.

In duplexed Central Controller systems, configuration data is kept duplexed on both Loggers. It is always resynchronized when a Logger is restarted.

*Script data* is also kept on both Loggers. Script data include all call routing and administrative scripts that the system software uses in call routing (both current and previous versions).

Historical and Real-time Data

Historical data and Real-time data provide information about certain objects in the system such as service, skill groups, and routes.

Real-time data provide current information on these objects.

Historical data fall into four categories: five-minute snapshots, interval summaries (15-minute or half-hour), call detail records, and events.

The five-minute tables contain *snapshot data*, which are values that are derived from real-time data. Snapshot data provides a view of contact center activity at a particular instant. Since the
five-minute values change frequently, they are not synchronized across the central databases of a duplexed Central Controller.

**See Also**

For the tables in which the Historical data and Real-time data are stored, refer to the *Database Schema Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*.

### Central Database

The central database on the Logger contains the following types of data:

- Full configuration information for the enterprise
- All routing scripts—current and, if you choose to save them, past versions
- Event data
- Call detail data
- Five-minute summary data
- Half-hour only historical data, which consists of application gateway, campaign, dialer skill group, network trunk group, physical controller, route, trunk group, and translation route data
- Interval historical data (15-minute or half-hour), which consists of agent, agent skill group, call type, call type skill group, campaign query rule, dialer, peripheral, service, and skill group data

The Unified ICM central database maintains five-minute summary and interval (15-minute or half-hour) historical data for each:

- Route
- Service
- Skill group
- Trunk group

It also maintains five-minute summary data for Routing Clients and Scripts data for Application Gateways and Network Trunk Groups. Although you can view these data in reports, you cannot modify them directly or indirectly.

For specific information on the tables of the Unified ICM databases, refer to the *Database Schema Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* or the online ICM Schema Help.
The central Unified ICM database resides with the Logger itself. If the Logger is duplexed, each physical Logger has its own copy of the database. If the Logger services multiple customers, each machine has a separate database for each customer.

The name of the central database has the form inst_sideX, where inst is an up-to-five-character instance name and X indicates the side of the central controller (A or B). For example, the central database for cus01 on the Side A Logger is named cus01_sideA.

Database Sizing and Creation

When you first set up the Logger software on a machine, you must also create the central database. If you set up multiple Loggers (for multiple customers), you must create a central database for each instance.

Before creating the database, you must determine how much space it requires. The size of the database depends on a number of factors, including the size of your configuration, the expected call load, how long you want to retain historical data, and the number and size of configured ECC variables.

Use the Database Sizing Estimator applet to estimate the database size, based on the expected usage.

Note: ECC variables add impact for each Route Call Detail (RCD) and Termination Call Detail (TCD) generated, which results in a large impact, so make sure this information is accurate. From this information, the Database Sizing Estimator applet can more accurately determine the impact of the specified ECC variables on the database size for the given number of retention days (usually 14 days for a logger database; larger number for HDS databases).

To prevent the database from growing indefinitely, old records are automatically purged from the historical tables on a regular basis. You can work with your Unified ICM support provider to decide how long you want to retain historical data in the central database.

For specific information on sizing and creating the database, see Chapter 4, "Database Administration (page 45)."

Optimization Tips for SQL Server 2005 with SP3

Note: Unified ICM/CCE/CCH Release 8.0(1) supports SQL Server 2005 with SP3 for new installs and upgrades. Systems with SQL 2000 must upgrade to SQL 2005 SP3 before upgrading Unified ICM.

SQL Server database files can be configured to grow automatically, using the Autogrow feature. This eliminates many problems that occur when logs or databases run out of space.

In the event that the Unified ICM database is undersized or there is an unplanned increase in the data stored in the database and the Unified ICM processes cannot purge the data to maintain the maximum database size, the autogrow option automatically expands the database when additional space is required.
See Also

For more information about autogrow, refer to the *Microsoft SQL Server System Administrator’s Guide*.

Database Updates and Changes

Each Administration & Data Server has a copy of the central database configuration data and scripts in its local database (awdb). All Configuration Manager tools and the Script Editor use the local database (awdb) copy to make changes to configuration and script data. These tools first modify the data in the Central Controller database, which is then copied to the local database (awdb). This ensures that the local database (awdb) copy is up-to-date with the central database. The Logger replicates historical data to the HDS database on the Administration & Data Server.

Local Database (AWDB)

The local database (awdb) contains the following information:

- Configuration information (copied from the central database), if the Administration & Data Server has a configuration role
- Scripts (copied from the central database)
- Real-time data

For specific information on the tables of the Unified ICM databases, refer to the *Database Schema Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* or the online ICM Schema Help.

Database Creation and Initialization

The local database (awdb) is created automatically and initialized when you install the Administration & Data Server software. Its name has the form inst_awdb, where inst is an up to five-character instance name. For example, the local database (awdb) for instance ins01 is named ins01_awdb.

Real-time Data

The real-time client process on the Administration & Data Server keeps the real-time data in the local database (awdb) up-to-date. The real-time data is updated in the local database (awdb) every ten seconds. Old real-time data is constantly overwritten by new real-time data.

See Also

For information on how real-time data is delivered, see Chapter 2, "Fault Tolerance (page 15)."
Configuration Management Service (CMS)

In integrated environments, the Configuration Management Service (CMS) coordinates the configuration of objects common to both the system software and to application instances. CMS also authenticates agents when they log in. Common objects are stored both in the application instance local database (awdb) and the Unified ICM central database. The copy of the data in the Unified ICM central database is used for integrated reporting and for authentication of agents. The copies of the data in the application instance databases are used for application specific reporting and for application operation.

CMS includes the following components:

- A set of client libraries that reside on the application instance system and are called by the application.
- A service process that runs on a Unified ICM Administration & Data Server.

The server process reads configuration data from the local database (awdb) and writes configuration data to Unified ICM via the Central Controller API (ConAPI).

The CMS client library communicates with the CMS server process using point-to-point communications. The ConAPI is exposed on the CMS client.

The following figure shows the CMS integrated architecture.

*Figure 9: CMS Integrated Architecture*

There might be multiple CMS services in a global Unified ICM system, just as there might be multiple Administration & Data Servers in a Unified ICM system.
Temporary Database

Because real-time or historical data are read frequently by the reporting clients that might have complex queries, the SQL Server uses the tempdb database to store the data result set before it is given to the connected clients. For better performance, set this database to **Auto Growth**.

Historical Data Server

Administration & Data Servers need to access historical data (15-minute and half hour data, call detail, and so forth). The system software normally stores historical data in the central database on the Logger, as well as on the Administration & Data Server that acts as the Historical Data Server (HDS).

One Administration & Data Server at each admin site is an HDS machine. The Central Controller forwards historical records to the HDS machine for storage in a special local database (awdb). Other Administration & Data Servers at the local site can retrieve historical data from the HDS machine without having to access the central site (see the following figure).

![Figure 10: Historical Data Server Architecture](image)

To set up an Historical Data Server, you must configure the Logger to perform historical data replication. You must also configure an Administration & Data Server to be an Historical Data Server. You can use the ICMDBA tool to create an HDS database, then use the Web Setup tool to add an Administration & Data Server with an HDS role.

Small to Medium Historical Data Server Deployments

**Note:** Before reviewing this section, review the *Cisco Unified Contact Center Enterprise 8.x Solution Reference Network Design (SRND)* at [http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html) for scalability details about small to medium deployments.
In this deployment, all agent-related historical data is replicated to an HDS.

This deployment type supports the following Logger setup:

- Maximum of 2 Loggers
- Maximum of 2 Historical Data Servers allowed per Logger side

There are three options available for an Administration & Data Server role in a small to medium deployment:

- **Administration Server, Real-time and Historical Data Server and Detail Data Server (AW-HDS-DDS):** Stores real-time, historical, call detail, and call variable data, including agent historical data filtered by peripheral

  This role is similar to the "Distributor AW with HDS" role in previous ICM releases. It provides ability for configuration changes as well as both real-time and historical reporting. The real-time and historical reporting is supported using one of two reporting clients: WebView server or Cisco Unified Intelligence Center (CUIC). The call detail and call variable data are supported for custom reporting data extraction to meet the requirements for System Call Trace tool and feed historical data to the CUIS (Archiver).

- **Administration Server and Real-time Data Server (AW):** Stores real-time data, including agent historical data filtered by peripheral, but no historical data

  This role is similar to the "Distributor AW" role in previous ICM releases. This role provides the ability for configuration changes as well as for real-time reporting. The real-time reporting is supported using either WebView server or Cisco Unified Intelligent Center (Reporting client). This role does not support historical reporting.

- **Configuration-Only Administration Server:** HDS is not enabled and real-time reporting is turned off. This deployment only allows configuration changes with no real-time and historical reporting.

**See Also**

Refer to the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for details about how to use the Web Setup tool to add Administration & Data Servers.

**Large Historical Data Server Deployments**

**Note:**


- This deployment is *not* supported in Unified SCCE; however, Unified SCCE Release 7.5 is supported in the 8.0(1) solution.
In this deployment, historical data can be distributed for scalability purposes.

This deployment type supports a maximum of 4 Historical Data Servers per Logger side, which can be configured as 3 AW-HDS and 1 HDS-DDS deployments (see descriptions below).

There are four options available for an Administration & Data Server role in a large deployment:

• **Administration Server and Real-time and Historical Data Server (AW-HDS):** Stores real-time and historical data, including agent historical data filtered by peripheral, but no call detail and call variable data

  This role provides ability for configuration changes as well as for both real-time and historical reporting. The real-time and historical reporting is supported using either WebView server or Cisco Unified Intelligent Center (Reporting client).

• **Historical Data Server and Detail Data Server (HDS-DDS):** Stores only historical data, including all agents and detail data (TCD, and so on) with additional indices (this option is limited to one per Logger side)

  This role provides support for historical reporting, Call Detail data extraction for System Call Trace tool and feed to CUIS Archiver. This deployment also includes configuration data available for historical reporting. Real-time data reporting and the ability to make configuration changes are not supported.

• **Administration Server and Real-time Data Server (AW):** Stores real-time data, including agent historical data filtered by peripheral, but no historical data

  This role is similar to the "Distributor AW" role in previous ICM releases. This role provides the ability for configuration changes as well as for real-time reporting. The real-time reporting is supported using either WebView server or Cisco Unified Intelligent Center (Reporting client). This role does not support historical reporting.

• **Configuration-Only Administration Server:** HDS is not enabled and real-time reporting is turned off. This deployment only allows configuration changes with no real-time and historical reporting.

**See Also**

Refer to the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for details about how to use the Web Setup tool to add Administration & Data Servers.

For specific information about setting up an HDS database, see Chapter 4, "Database Administration (page 45)."

### ChangeStamps and Locks

To prevent users from changing the same data simultaneously, Unified ICM configuration data records contain a ChangeStamp field. The ChangeStamp field is incremented when the record is changed in the central database. When an administrator makes changes to configuration data and sends the changed data to the Logger, the value of the ChangeStamp field is compared to
the value in the Logger’s copy. If the values differ, this means that another administrator has changed the data in the interim. The Logger rejects the change, and the administrator is notified to refresh the data view and try again.

The system software also provides the Master lock, solely for compatibility with previous Unified ICM releases. The Master lock provides exclusive access to all configuration data and scripts. If a user holds the Master lock, no one can acquire any other locks. You must explicitly acquire and release the Master lock through Lock Admin. Use one of the more specific lock types instead.

The Lock Admin tool (accessible through the Administration & Data Server or Administration Client) displays the status of all locks:

Figure 11: Lock Admin Tool

To release a lock:

1. Select the lock by clicking on its name in the Type column.
2. To release the lock, select Release.
Database Administration

When you install a new Logger, you must create its central database. When you create a database, you must specify the size of its data or log file (or files). The data file (or files) size should be sufficient for all the data you expect the database to hold.

The size of the central database depends on the size of your call center, your expected call load, and your specific data retention requirements. Based on your expectations and requirements, you can create a central database of the appropriate size.

You must create an HDS database on a real-time Administration & Data Server. The same considerations that affect the size of the central database also affect the size of the HDS database.

Over time, the size of your enterprise or your call volumes might change significantly. Therefore, you might need to resize the central and HDS databases to meet new requirements.

This chapter presents the ICM Database Administration (ICMDBA) tool, the Database Sizing Estimator applet, and the Database Retriever dialog, that give you the capability to manage your Logger and local databases (awdb).

This chapter contains the following topics:

- Overview, page 46
- Retaining Historical Data, page 46
- Database Administration Tool, page 47
- Database Sizing Estimator Web Applet, page 58
- Setting Up an Administration & Data Server with an Historical Data Server, page 60
- When a Database Nears Capacity, page 61
- Monitoring the Database Size, page 62
- Allocating Additional Space, page 63
- Initializing the Local Database (AWDB), page 63
Overview

The local database (awdb) contains configuration and real-time data, if the Administration & Data Server role includes a real-time server. Because the real-time data in the local database (awdb) are constantly overwritten by new data, the database size remains fairly constant. You normally do not need to resize the local database (awdb). If you do need to resize the local database (awdb), you can do so using the ICM Database Administration (ICMDBA) tool. The procedures for using the ICMDBA tool are described later in this chapter.

The data in the central database and HDS database grow as they accumulate historical data and call detail records. The growth is directly related to the following factors:

- Size of the Unified ICM configuration; for example, how many services, skill groups, routes, and trunk groups are configured.
- Call rate; that is, how many calls per day the system software is handling.
- How long historical data is kept in the database.

The amount of configuration data directly affects the amount of historical data generated. The system software generates a new historical record every half hour for each service, skill group, route, trunk group, etc., configured in the Unified ICM system.

You must size and create the central and HDS databases after installing the system software. Use the Database Sizing Estimator applet for estimating the size of these databases, based on the expected usage. (See the "Database Sizing Estimator Applet (page 58)” section for more details.)

The database size remains adequate as long as your usage is consistent with the values used to size the database. If your configuration expands significantly or if you change the retention times for historical data, you might have to increase the size of the database. This might involve adding additional disks to the system.

Normally, the central database transaction logs are sized to handle the processing of historical data at a call rate of 35 calls per second.

Retaining Historical Data

The system software initiates a purge process on the Logger once every day. By default, the purge process runs each night at 12:30 A.M. The purge process deletes records that are older than a specified number of retain days. When you set up the Logger using the Web Setup tool, you can modify the default retention time and purge schedule.

The following data lists the default settings for retaining historical data.
Table 1: Logger Database Historical Tables

<table>
<thead>
<tr>
<th>Historical Tables</th>
<th>Default Retention Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logger_Admin, Import_Rule_History, Persistent</td>
<td>30 days</td>
</tr>
<tr>
<td>Recovery</td>
<td>100 days</td>
</tr>
<tr>
<td>All other historical tables</td>
<td>14 days</td>
</tr>
</tbody>
</table>

As of Release 7.5(1), though the above table remains accurate, the following large historical tables are not purged by the system software but as a scheduled SQL Server Agent Job:

- Agent_Event_Detail
- Call_Type_SG_Interval
- Dialer_Detail
- Network_Event_Detail
- Route_Call_Detail
- Route_Call_Variable
- Termination_Call_Detail
- Termination_Call_Variable

Caution: SQL Server Agent Jobs are installed and enabled during the upgrade procedure. These jobs should not be stopped while the system software is active. However, if the logger and Administration & Data Server-hds component services are to be stopped for any maintenance that will require more than one day, the SQL Server jobs must be manually disabled using the SQL Server enterprise management tool. Later, once the services are started, re-enable the jobs.

Database Administration Tool

The ICMDBA tool (icmdba.exe) is included with the system software and is located in the \icm\bin directory. This tool provides a central utility that allows you to manage Unified ICM database administration. Use this tool to:

- Create, edit and delete central databases, local databases, and historical database for installed Unified ICM customers
- Resize database files
- Recreate a database
- Import/export Unified ICM configuration data to/from databases
- View database properties
In addition to these tasks, you can use the ICMDBA tool to start or stop a server, and to do some limited SQL Server configuration.

**Note:**

- Before using the ICMDBA tool, the system software for a customer must be installed. Refer to the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*, for information on the Unified ICM installation.

- The ICMDBA Import/Export feature pertains to Unified ICM configuration data only. To import or export Unified ICM historical data, use Microsoft’s SQL Server Database Backup and Database Restore utilities.

---

### Starting ICMDBA

The following steps describe how to start ICMDBA.

**Note:** For detailed ICMDBA components field descriptions, refer to the online help.

**Step 1**

Start the ICMDBA tool either by double-clicking **ICMdba** in the Unified CCE Tools folder or by selecting **Start > Run > ICMDBA**.

**Step 2**

The ICMDBA main window displays.

*Figure 12: ICMDBA Main Window*

![ICMDBA Main Window](image)

The main window is a tree hierarchy displaying the Unified ICM database servers in the current domain.
**Note:** If you cannot find the server you want in the main window, you can select any computer on your local network by choosing **File > Add Computer** from the menu bar.

You can expand the server by clicking on the plus sign (+) next to its name. This displays the Unified ICM instances that have databases on the server. Expanding the Unified ICM instance displays a specific Unified ICM node or nodes (Administration & Data Server and Logger) on machines that have databases for that instance. Expanding the node displays the databases associated with the node. Expanding the node database displays a list of the individual tables in the node database. Under databases are the table groups, and the final level lists the tables in the group.

Databases can be created for instances with configured components or without configured components. When an instance does not have any configured components, database creation occurs under the instance within a *component placeholder* on the ICMDBA main window's application tree view. See the "Creating a Database Without Configured Components (page 50)" section for more information.

To view the properties of a table, right-click the desired table in the list and select **Properties** from the pop-up menu, or double-click the table in the list.

There are two ways to access the ICMDBA tool functions:

- From the main window, select a node or database from the tree and then select a function from the menu bar menu.
- Right-click a node or database to display a pop-up menu.

---

### Creating a Database With Configured Components

Use the Create function to create a database for an Administration & Data Server or Logger. You can only create one Logger database per side.

To create a new Unified ICM database:

**Step 1**
With the system software running, for the server and instance, select the node (Administration & Data Server or Logger) where you want to create the database.

**Step 2**
Select **Database > Create** from the menu bar (or click the right mouse button and select **Create**). The Create Database window displays.

**Step 3**
Enter the following information for the database:

- **DB Type.** Specify the type of database: **Outbound Option** for an outbound dialer, **Administration & Database Server** for a local database (awdb), or **Historical Data Server/Detail Data Server (HDS/DDS)** for Administration & Data Server machines. For a **Logger** device, the default database type displays (Logger side must be selected).

- **ICM Type.** Specify whether this is a Unified ICM or Unified CCE Enterprise, Unified ICMH, or CICM (Customer ICM) system.
- **Region.** Specify regional information where applicable.

- **Partitions.** If partitioning is enabled, check this box and specify the maximum number of partitions allowed for the customer (1 through 5).

  **Note:** Partitioning on new installations is no longer supported and is no longer provided as a checkbox option from the Web Setup windows; that is, you cannot create new partitioning on a server. Although the partitioning checkbox has been removed, upgrading to 8.0(1) does not automatically remove partitioning on an existing system.

**Step 4**  
Select **Add.** This button invokes the Add Device window.

Use this window to create a new data file and a new log file for the selected database. Specify the disk drive letter and size in megabytes for each new file.

When finished adding the file, select **OK** to return to the Create Database window.

**Note:** By default, the newly created data file will be set to "Automatically Grow," should it exceed the initially specified size. This setting, as well as the maximum file size, can be modified using SQL Server Enterprise Manager.

**Step 5**  
When you have completed entering information in the Create Database window, select **Create** to close the window and create the database.

**Note:** Partitioning is only supported for customers using Unified ICM. It is not supported in Unified ICMH, Unified CCE, or Unified CCH.

---

**Creating a Database Without Configured Components**

Use the Create function to create a database for an Administration & Data Server or Logger. You can only create one Logger database per side.

**Note:** When an instance does not have any configured components, database creation occurs under the instance within a *component placeholder*.

To create a new Unified ICM database:

**Step 1**  
With the system software running, for the server and instance, select the *instance* where you want to create the database.

**Step 2**  
Select **Database > Create** from the menu bar (or click the right mouse button and select **Create**). The Select Component dialog displays.

**Step 3**  
Select the **Administration & Data Server, LoggerA,** or **LoggerB** component and select **OK.**

**Step 4**  
If you select LoggerA or LoggerB, the Select Logger type dialog displays, where you can select **Enterprise,** **CICM,** or **NAM.** Select the logger type and select **OK.**

**Step 5**  
The Create Database window displays.
Enter the following information for the database:

- **DB Type.** Specify the type of database: **Outbound Option** for an outbound dialer, **Administration & Database Server** for a local database (awdb), or **Historical Data Server/Detail Data Server (HDS/DDS)** for Administration & Data Server machines. For a **Logger** device, the default database type displays (Logger side must be selected).

- **ICM Type.** Specify whether this is a Unified ICM or Unified CCE Enterprise, Unified ICMH, or CICM (Customer ICM) system.

- **Region.** Specify regional information where applicable.

- **Partitions.** If partitioning is enabled, check this box and specify the maximum number of partitions allowed for the customer (1 through 5).

**Note:** Partitioning on new installations is no longer supported and is no longer provided as a checkbox option from the Web Setup windows; that is, you cannot create new partitioning on a server. Although the partitioning checkbox has been removed, upgrading to 8.0(1) does not automatically remove partitioning on an existing system.

Select **Add.** This button invokes the Add Device window.

Use this window to create a new data file and a new log file for the selected database. Specify the disk drive letter and size in megabytes for each new file.

When finished adding the file, select **OK** to return to the Create Database window.

**Note:** By default, the newly created data file will be set to "Automatically Grow," should it exceed the initially specified size. This setting, as well as the maximum file size, can be modified using SQL Server Enterprise Manager.

When you have completed entering information in the Create Database window, select **Create** to close the window and create the database.

**Note:** Partitioning is only supported for customers using Unified ICM. It is not supported in Unified ICMH, Unified CCE, or Unified CCH.

Use the Delete function to delete a Administration & Data Server or Logger database.

**Note:** When an instance does not have any configured components, *component placeholders* display under that instance on the application tree view; therefore, when the database is deleted the component placeholders no longer display.

To delete a database:

With the system software running, for the server, instance, and node (Administration & Data Server or Logger), select the database that you want to delete.
Step 2 Select **Database > Delete** from the menu bar.

Step 3 The Delete Database prompt displays. Select **Yes** to delete the database (or **No** to return to the main window). Another message displays to verify that you want to delete the database. Indicate whether or not to delete the database.

Step 4 Select **Close** to exit. Check the main window to verify that the database was deleted.

---

### Expanding a Database

Use this function to add a new storage file.

**Note:** ICMDBA allows a database to be expanded a maximum of 49 times (resulting in 50 segments). In the event that you reach this limit, you must either recreate the database or use SQL Enterprise Manager to modify the database.

To expand database storage on a storage device:

**Step 1** For the server, instance, and node (Administration & Data Server or Logger), select the database that you want to expand.

**Step 2** Select **Database > Expand** from the menu bar (or click the right mouse button and select **Expand**).

**Step 3** The Expand Database window displays.

*Figure 13: Expand Database Window*

Use the window to adjust the size allocation on the database's storage device, by completing the following fields:

- **Component**. Specifies whether the file is a data file or log file. Each database must have a file for each type of service.
• **Available Drives.** Specify the drive on which to create the database.

• **Size.** Specifies the size (in MB) of the storage. Field displays a default size. This field can be edited to adjust size as necessary.

**Step 4** Select **OK** to expand the file and exit the screen.

---

**Recreating a Database**

Use the Recreate function to recreate a database. The procedure for recreating a database is the same as when you create a database.

**Note:**
- When you recreate a database, the information currently stored in the database is deleted.
- When an instance does not have any configured components, database creation occurs under a *component placeholder* on the application tree view.

To recreate a database:

**Step 1** For the server, instance, and node (Administration & Data Server or Logger), select the database that you want to recreate.

**Step 2** Select **Database > Recreate** from the menu bar. The Recreate Database window displays.

**Step 3** Enter the database information. See the **Creating a Database (page 49)** section for a description of the fields.

**Step 4** Select **Create** to continue. A message displays asking if you are sure you want to recreate the database. Select **Yes** to continue the operation.

**Step 5** The next Recreate Database window displays. Select **Start** to recreate the database. When the process is completed, a message displays indicating the action was successful. Select **OK** and then select **Close** to exit.

---

**Viewing Database Properties**

The ICMDBA tool allows you to view the properties of specified databases.

To view the properties of a database:

**Step 1** For the server, instance, and node (Administration & Data Server or Logger), select the database that you want to view.

**Step 2** Select **Database > Properties** from the menu bar (or click the right mouse button and select **Properties**). The Properties window displays.
The screen display includes the following information:

- Instance name
- The database configuration
- The size and percentage of the combined files
- The size of the data and log files

**Step 3** When you are finished viewing the database properties, select **Close** to exit the window.

---

**Viewing Table Properties**

ICMDBA also allows you to view the properties of each table in the database.

To view the properties of a table:

**Step 1** Select and expand the database to display the tables of a database.

**Step 2** Double-click the table you want to view. The Properties window for the table displays.

**Step 3** When you are finished viewing the table properties, select **Close** to exit the window.

---

**Importing/Exporting Data**

You can use Import/Export functions to import/export Unified ICM configuration data from one database to another.

**Note:** The ICMDBA Import/Export feature pertains to Unified ICM configuration data only. To import or export Unified ICM historical data, use Microsoft’s SQL Server Database Backup and Database Restore utilities.

To import/export data:

**Step 1** For the server, instance, and node (Administration & Data Server or Logger), select the database from which you want to import/export data.

**Step 2** Select **Data > Import** (or **Export**) from the menu bar. The Import (or Export) window displays.

**Step 3** Check **Lockout Changes**, if you want to ensure that changes cannot be made to the database during the import or export operation.

**Step 4** Check **Truncate Config Message Log**, if you want to truncate the Config_Message_Log table in the Logger database.

**Note:** Truncating deletes the data and does not export the Config_Message_Log table.
Step 5  Indicate the path for the source/destination of the data.

Step 6  Select Import/Export to display the next Import/Export window.

Step 7  Select Start to import/export the data. When the process is completed, a message displays indicating the action was successful. Select OK and then select Close to exit. You can select Cancel at any time to end the process.

Synchronizing Database Data

Use the Synchronize function to synchronize the data of two Logger databases.

To synchronize databases:

Step 1  For the server and instance, select the Logger database to synchronize.

Step 2  Select Data > Synchronize from the menu bar. The Synchronize window displays.

Step 3  Check Lockout Changes, if you want to ensure that changes cannot be made to the database during the synchronize operation.

Step 4  Check Truncate Config Message Log, if you want to truncate the Config_Message_Log table in the Logger database.

Step 5  Select the server name and database for both source and target from the drop down lists. To select a server that is not on the drop down list, select Add and enter the server name in the Add Server box.
Step 6  Select **Synchronize**.

Step 7  A message box appears asking for confirmation. Select **OK** to continue.

Step 8  The next Synchronize window displays. Select **Start** to import/export the data. When the process is completed, a message displays indicating the action was successful. Select **OK** and then select **Close** to exit. You can select **Cancel** at any time to end the process.

Configuring the Server

ICMDBA allows you to start or stop a server and to do some limited server configuration.

To start or stop a server, select the node from the list and select **Server > Start/Stop** from the menu bar.

To configure a server:

Step 1  Select the server and select **Server > Configure** from the menu bar. The Configure window displays.
Step 2  Use this window to modify the following SQL Server parameters:

- **User Connections.** Indicate the maximum number of users that can connect to SQL Server at one time.

- **Locks.** Indicate the maximum number of available locks.

- **Open Objects.** Indicate the maximum number of available open objects.

  **Note:** User Connections, Locks, and Open Objects are "dynamically allocated" by SQL Server. Unified ICM does not allow you to change these options, so they are grayed out.

- **Open Databases.** Indicate the maximum number of available open databases.

  **Note:** Open Databases is not available in SQL 7.0 or SQL 2000.

- **Memory.** Indicates the amount of memory (in megabytes) allocated to SQL Server processing.

  **Note:** Memory can be configured to be a specific value instead of the SQL Server default of "Dynamic." Specifying a value of 0 can set the Memory setting to "Dynamic."

- **Recovery Interval.** This setting controls checkpoint frequency.

- **Max Async ID.** Indicates the maximum number of outstanding asynchronous disk input/output (I/O) requests that the entire server can issue against a file.

  **Note:** Max Async ID is not available in SQL 2000.

Step 3  When you are finished configuring the server, select **OK** to complete the operation or select **Cancel** to end the operation without making any changes.
Note: When you use the **Configure** option, the SQL Server, Administration & Data Server and Logger restart automatically. However, when you use the Stop option from the Server menu, the Logger and Administration & Data Server must be manually restarted from ICM Service Control.

**Database Sizing Estimator Web Applet**

The Database Sizing Estimator web applet allows you to perform your database sizing needs.

Note: The Database Sizing Estimator estimates databases for Unified ICM Release 7.5(1) or higher.

When this applet initially runs, it provides initial values typical for a small installation.

Note: The Database Sizing Estimator runs locally as a Java Applet on your own system. The information you enter into this applet is not sent back to the web server hosting the applet.

The Database Sizing Estimator estimates the storage requirements for a Cisco Unified ICM, Unified CCE, or Unified SCCE logger or HDS database given information about the environment's configuration (for example, the number of agents, skill groups, call types, and so on) and database retention days. You can supply initial values by loading values from your local Unified ICM database.

Whenever values are updated in the Database Sizing Estimator, the application recalculates its totals, allowing you to immediately see the affects of each change as it is being made, with the values displayed in a spreadsheet. This allows you to engage in what-if type scenarios to see the effects that various changes will have on the database sizing requirements.

The Database Sizing Estimator allows you to save the values as an XML file on your local machine. At any time, the saved XML file can be loaded back into the Database Sizing Estimator, so you can continue revising your estimates.

**Starting Database Sizing Estimator**

The following steps describe how to start the Database Sizing Estimator.

Note: For Database Sizing Estimator field-level descriptions, refer to the online help.

**Step 1**
Open the Database Sizing Estimator applet by either selecting **Database > Estimate** in the ICMDBA tool or by entering the following URL in a web browser window: [http://www.cisco.com/web/applicat/dbest801/DBEstimator.html](http://www.cisco.com/web/applicat/dbest801/DBEstimator.html).

**Step 2**
The Cisco Unified ICM/Unified CCE/Unified SCCE Database Sizing Estimator window displays.
Step 3

The window displays initial default values for all fields. As you change the field values, the database size requirements are updated in real time. Values can be loaded from a previous version or from the Cisco Unified ICME/CCE/SCCE Database Retriever dialog (page 60) by selecting Load from File to load an external XML data file.

Estimating the Size of a Database

Use the Database Sizing Estimator applet for the following:

- Estimate required database size
- Control the amount of time that data is retained
- Save a database estimate to a file
- Open a previously saved database estimate file

To estimate a database, perform the following steps.

Note: Steps one through three in the following procedure only apply when using existing databases.
Step 1  Use your existing database as the starting point. Select **Load from DB** in the Database Sizing Estimator's main window. The Cisco Unified ICME/CCE/SCCE Database Retriever dialog (page 60) displays.

Step 2  Select the database you want to use as the starting point for your sizing estimates.

Step 3  Select **Retrieve**. The fields auto-populate the information in the Database Sizing Estimator's main window.

Step 4  Modify the database information depending on your scenario. As changes are made, the Database Size Required value changes.

Step 5  Save your work in progress by selecting **Save to File**.

**See Also**

Refer to the Database Sizing Estimator online help for more information.

---

**Cisco Unified ICME/CCE/SCCE Database Retriever Dialog**

The Cisco Unified ICME/CCE/SCCE Database Retriever dialog, which is accessed from the Database Sizing Estimator applet, queries the existing database and registry configuration. The Database Sizing Estimator applet then uses this data to provide values, which can be modified.

To access the Database Retriever dialog, select **Load from DB** in the Database Sizing Estimator applet on your local machine.

**Note:** Cisco Unified ICME/CCE/SCCE Database Retriever can retrieve the configuration and retention information from any Unified ICME, Unified CCE, or Unified SCCE system containing a Logger or Historical Data Server (HDS) database at Release 7.0 or higher. However, the calculations performed only apply to the estimated database size for that database when running Unified ICME, Unified CCE, or Unified SCCE at Release 7.5(1) or higher, depending on the value indicated in the Schema Version drop-down list. Therefore, the Database Sizing Estimator can calculate a database size for a newer schema other than the system where the Database Sizing Estimator is connected.

**See Also**

Refer to the Database Sizing Estimator online help for more information.

---

**Setting Up an Administration & Data Server with an Historical Data Server**

There are two ways to set up an Historical Data Server (HDS) machine:

- **Where the instance is created in the domain, but is not already added** (page 61)
- **Where the instance is created in the domain and is already added** (page 61)
Setting Up HDS Machine When Instance Is Created, Not Added

Perform the following steps to create the HDS machine.

**Step 1** Run the Cisco Unified ICM/Contact Center Enterprise & Hosted Installer (if it has not already been run) on the local machine.

**Step 2** Run the Web Setup tool for that machine (in a browser, from anywhere). Under **Instance Management**, select **Add** and add the instance.

**Step 3** Run the ICMDBA tool on the local machine. Create the Historical Data Server/Detail Data Server database.

**Step 4** Return to the Web Setup tool. Under **Component Management**, select **Add** on the Administration & Data Server list page, then follow the instructions in the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*. If you did not perform step 3, the Administration & Data Server Add wizard will not allow you to finish this procedure until you create an HDS database.

Use the Database Sizing Estimator applet to determine the size of the database and the ICMDBA tool to create the database. (See the "Estimating the Size of a Database (page 59)" section and the "Creating a Database (page 49)" section.)

Setting Up HDS Machine When Instance Is Created, Already Added

Perform the following steps to create the HDS machine.

**Step 1** Run the ICMDBA tool on the local machine. Create the Historical Data Server/Detail Data Server database.

**Step 2** In the Web Setup tool, under **Component Management**, select **Add** on the Administration & Data Server list page, then follow the instructions in the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*. If did not perform step 1, the Administration & Data Server Add wizard will not allow you to finish this procedure until you create an HDS database.

Use the Database Sizing Estimator applet to determine the size of the database and the ICMDBA tool to create the database. (See the "Estimating the Size of a Database (page 59)" section and the "Creating a Database (page 49)" section.)

When a Database Nears Capacity

The system software has automatic checks to prevent the central database from becoming full:
• **Warning message.** When the central database begins to approach its capacity, the system software issues a warning message. By default this occurs when the database is 80% full, but this value can be configured.

Warning messages trigger an event that is registered in AlarmTracker, which displays in an EMS trace message in the console window.

• **Automatic purge.** If you select the Automatic Purge Adjustment option when you install the Logger software, the system software automatically deletes the oldest historical data when database usage exceeds 80% threshold and/or when the central or HDS database nears its capacity. If the data has not exceeded the retention period, it does not get deleted. By default, automatic purge occurs when the database is 80% full, but you can set the percentage when you set up the Logger. You can also set the retention period for data when you set up the Logger.

  **Note:** Refer to the Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted for more on purging information from databases.

• **Emergency Purge.** By default, the system automatically deletes oldest historical data from all historical tables when the database exceeds 90% usage capacity.

The automatic purge ensures that the database can never become completely full, which means that you will begin to lose older historical data.

### Monitoring the Database Size

You should regularly monitor the space used by the central database and transaction logs. You can monitor database size by viewing the Logger’s per-process log files. The per-process log files contain specific information on Logger and database activity. The following example shows a per-process event log file for a side A Logger.

![Figure 18: DUMPLOG Example of Per-Process Event Log File](image)

The Logger logs events and trace messages that show the percentage of space used in the database. These files are stored in a \logfiles subdirectory in the Logger’s directory (1a or 1b). You can view the Logger’s per-process log files by using the Unified ICM dumplog utility.
When the database becomes 80 percent full, the Logger logs an EMS warning message to the central database. The "80 percent full" warning message might also immediately be sent to your Unified ICM network management station via SNMP or SYSLOG.

**Note:** Refer to the *Serviceability Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for more information on using the dumplog utility.

If you decide that you need additional database space, contact your Unified ICM support provider.

### Allocating Additional Space

If the central database is growing too large, you might have to allocate additional space. Your Unified ICM support provider might have options for allocating more space, including:

- Remotely adding database space (if current disk space allows).
- Installing "hot-plugable" disk drives and configuring the disks while the system is running.

If you require additional space in the central database, you must back up the master database before more space is added.

**See Also**

For more information about backing up the database, see Chapter 5, "General Administration (page 65)."

### Initializing the Local Database (AWDB)

It should not be necessary to initialize the local database (awdb), since it is done automatically when the local database (awdb) is created. However, if you should ever need to initialize it again after it is first installed, you can do so.

To initialize the local database (awdb):

**Step 1** Double-click **Initialize Local Database** within the Administration Tools folder. The Initialize Local Database main window appears.

**Step 2** Select **Start** to transfer the data. As data are copied, the screen displays the number of rows processed for each table.

**Step 3** When the transfer is completed, select **Close** to exit.
General Administration

Because Unified ICM is a mission-critical application that runs 24 hours a day, the system software takes care of many routine administration tasks automatically. In general, the system software retains control of most of the database administration functions in order to keep external interference to a minimum.

This chapter describes the data integrity checks that the system software performs on configuration data. It also describes the scheduled database maintenance jobs that run automatically.

As the Unified ICM administrator, you might be responsible for performing several optional Unified ICM administration tasks:

• Setting networking options
• Monitoring Logger activity
• Backing up the central database
• Restoring the central database from backup
• Comparing databases
• Resynchronizing databases

This chapter describes each of these administration tasks.

Note: In order to conserve system resources, minimize all Unified ICM process windows prior to configuring your system.

This chapter contains the following topics:

• Built-In Administration, page 66
• Optional Administration, page 66
Built-In Administration

The system software maintains a database on each side of the Central Controller and the local database (awdb). Each database consists of a group of interrelated tables. As you add or update data in the database, you must ensure that logical relationships are maintained. For example, if you delete a trunk group, you must not leave trunks in the database that reference that trunk group. If you do, the integrity of the database is broken.

Configuration Manager prevents you from making certain changes that disrupt the integrity of the data in the database. However, it cannot prevent all such changes. Usually, if data integrity in the local database (awdb) is temporarily disrupted, no major problems occur. However, integrity problems in the central Unified ICM database could cause errors in system processing.

**Note:** To protect the integrity of the Unified ICM databases, do not use third-party tools to modify them. These tools do not protect against disruptions of database integrity. (You can use third-party tools to view Unified ICM data.)

When your Unified ICM support provider installs the Unified ICM system, they perform integrity checks to make sure that the database is configured correctly. After that, the integrity of the central database is maintained by the system software. You do not need to manually check the integrity of the Unified ICM central database. If you ever have a problem with data integrity in the central database, the problem is most likely a software problem that needs to be addressed by your Unified ICM support provider.

**Caution:** Any manual integrity checks of the central database must involve your Unified ICM support provider. Do not run the DBCC CHECKDB procedure on the central database while the Unified ICM system is running. This procedure will stop the Logger.

Optional Administration

You can perform optional administration functions for the system software such as manually checking data integrity in the local database (awdb), monitoring central database space, and viewing a Logger’s event logs. These tasks are not required, but you might find them useful in situations when you need to check the system immediately.

Checking Data Integrity in the Local Database (AWDB)

You can manually check the integrity of data in the local database (awdb). Configuration Manager provides a **Check Integrity** option under the Administer menu. Configuration Manager allows you to select which checks you want to execute.
To check data integrity at any time:

**Step 1** Invoke Configuration Manager by double-clicking its icon in the Administration Tools folder.

**Step 2** Select **Configure ICM > Administration > Integrity Check** from the menu bar. The following dialog box appears:

*Figure 19: Integrity Check Dialog Box*

**Step 3** Select specific checks to execute, or select **All** to perform all the checks.

**Step 4** Select **Start** to perform the checks. If any integrity problems are found, Configuration Manager displays a message describing the problems.

**Step 5** When you have performed all the checks you want, select **Done** to dismiss the Integrity Check dialog box.

The specific data integrity check procedures are listed in the following table.

**Table 2: Local Database Data Integrity Check Procedures**

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>Checks for the value NULL in specific fields in the database that must not be null. It also checks that the value of the RoutingClient.PeripheralID is NULL for routing clients associated with a NIC.</td>
</tr>
<tr>
<td>Targets</td>
<td>Checks for appropriate relationships among peripherals, targets at peripherals (services, skill groups, agents, and translation routes), trunk groups, network targets, announcements and peripheral targets.</td>
</tr>
<tr>
<td>Routes and Numbers</td>
<td>Checks that ID fields cross-referenced from several tables correspond to existing records.</td>
</tr>
<tr>
<td>Scripts</td>
<td>Checks for valid cross-references among scripts, call types, and dialed numbers.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>Checks for valid cross-references among enterprise services and services, and between enterprise skill groups and skill groups. Also performs several other checks on skill groups, trunks, etc.</td>
</tr>
</tbody>
</table>
### Procedure

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Adherence</td>
<td>Checks for valid relationships between agents and skill groups, between skill groups and services, between labels and routing clients, between dialed numbers and routes, and between peripherals and routing clients.</td>
</tr>
<tr>
<td>Names</td>
<td>Checks for invalid characters in enterprise names (EnterpriseName field) in various database tables. Enterprise names provide unique character-string names for objects in the Unified ICM configuration.</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Checks rules for Outbound Option Configuration.</td>
</tr>
</tbody>
</table>

For more information on the specific fields checked by these procedures, see the online help for the Configuration Manager tool.

### Viewing Logger Events

You can view recent Logger activity by viewing the Logger’s per-process log files. Per-process log files document events for the specific processes running on a computer. These files are useful in diagnosing problems with processes on the Logger (and on other nodes in the Unified ICM system).

You can also view Logger event data in the central database. The Event Management System (EMS) logs events to the central database. You should be especially aware of Error and Warning events generated by the Logger. For example, the system software logs a Warning event when the central database becomes 80% full.

**See Also**

Refer to the *Serviceability Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for more information on viewing the per-process log files and central database event data.

### Database Networking Support

You can use the SQL Server Setup program to specify which network protocols the database manager supports.

The correct order and states are:

1. **Shared Memory**: Enabled
2. **Named Pipes**: Enabled
3. **TCP/IP**: Enabled
4. **VIA**: Disabled
See Also

Refer to the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 8.x(y)* for detailed information about installing SQL Server.

For more information about database networking, refer to the *Microsoft SQL Server System Administrator’s Guide*.

Manual Intervention to Restart Cisco Unified Intelligent Contact Management Processes After an Exception

Sometimes, manual intervention is required to restart Unified ICM processes after an exception. This error can be suppressed by setting a registry value.

Windows allows you to change the handling of hard error popups that result from application and system errors. Such errors include no disk in the drive and general protection (GP) faults.

Normally, these events cause a hard error popup to be displayed, which requires user intervention to dispatch. This behavior can be modified so that such errors are logged to the Windows event log. When the error is logged to the event log, no user intervention is necessary, and the system provides a default handler for the hard error. You can examine the event log to determine the cause of the hard error.

**Note:** The "hard errors" referred to in this section could be critical system errors, such as an I/O error, no disk in drive, and so on. These system errors result in a dialog box that pops up on the window’s console and requires manual intervention by a user. Handling of these types of system errors (dialog box popup or event log) is controlled by the registry setting listed below.

The following registry entry controls the hard error popup handling in Windows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows\ErrorMode
```

The following are valid values for ErrorMode:

- **Mode 0**: This is the default operating mode that serializes the errors and waits for a response.

- **Mode 1**: If the error does not come from the system, this is the normal operating mode. If the error comes from the system, this logs the error to the event log and returns OK to the hard error. No intervention is required and the popup is not seen.

- **Mode 2**: This always logs the error to the event log and returns OK to the hard error. Popups are not seen.

If you want to suppress the Windows exception, set the registry key value to 2 for the "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows\ErrorMode" registry key.
Backup and Restore

A database can be lost or corrupted for several reasons, such as:

- Disk drive failure
- Bad media
- Software error (in the Database Manager or elsewhere in the system)

Because you cannot protect against all these conditions, you must have a backup strategy in place. This is especially important if you have a simplexed central database configuration. However, even for a duplexed system, you still need to perform backups to protect against software problems that corrupt both sides of the system.

Database

The following database backup strategies are commonly used:

- Regularly scheduled database backups
- Mirrored disk configurations
- Redundant Array of Inexpensive Disks (RAID) configurations

Although the last two strategies might decrease system performance, they have the advantage of not requiring manual intervention. However, while these configurations protect against disk drive failure and bad media, they might not protect against some software errors.

In a simplexed database configuration, you need to ensure protection against all types of errors. To protect your data, regularly back up the central database.

To perform a database backup, use the SQL Administrator tool provided with SQL Server.

**Note:** The SQL Monitor service must be running during a backup. If SQL Server is not configured to start SQL Monitor automatically, you must start the service manually before beginning the backup.

When you restore a database, you can only restore up to the last backup. Any transactions after that backup are lost. Therefore daily backups are recommended for simplexed systems.

**Note:** You must backup the entire database at each backup interval. The system software does not support the use of transaction log dumps as incremental backups.
See Also

For general information about developing a backup strategy, including the use of mirrored disks, refer to *Microsoft’s SQL Server System Administrator’s Guide*.

For specific information about backing up a database using SQL Administrator, refer to *Microsoft’s SQL Administrator User’s Guide*.

Best Practices for Performing a Backup

To backup an Unified ICM database:

- Stop Unified ICM services for the processes that are using the database being backed up.
- Run the backup.
- Restart Unified ICM services after the backup completes.

*Note:* On a duplexed system, calls will continue to be processed if sideA is backed up at a different time than sideB.

Comparing Databases

For diagnostic purposes, you might want to check that two databases have the same data in a specific table. For example, you might want to check that the ICM_Locks table contains the same data on both sides of a Central Controller. The tool dbdiff.exe performs this type of check. Its syntax is as follows:

```
dbdiff database1.table@host1 database2.table@host2
```

For example:

```
dbdiff cust1_sideA.ICM_Locks@geoxyzlgra cust1_sideB.ICM_Locks@geoxyzlgrb
```

The batch script diffconfig.bat invokes dbdiff for various tables to automatically compare two Unified ICM databases. Its syntax is as follows:

```
diffconfig database1 host1 database2 host2
```

For example:

```
diffconfig cust1_sideA geoxyzlgra cust1_sideB geoxyzlgrb
```

Resynchronizing Databases

It might occasionally be necessary to repair a corrupt Logger database on one side of a duplexed Unified ICM by copying the Logger database from the other side. You can synchronize the
databases using either the DOS Command window or the ICM Database Administration (ICMDBA) tool.

**Note:** Cisco recommends performing these procedures in a maintenance window.

### Synchronizing Databases from the Command Window

The following directions explain how to perform this copy from side A to side B for a customer named CustX.

To copy CustX database from Side A to Side B:

**Step 1** Stop the Side B Logger, if it is running.

**Step 2** In a DOS Command window on the Side B Logger, change to the \icm directory.

**Step 3** Run the following command:

```
install\syncloggers geoCustXlgrA CustX_SideA geoCustlgrB CustX_SideB.
```

**Step 4** When prompted, verify that the configuration will be deleted from the correct database and type **Y** to continue.

When the command completes, you can restart the side B Logger.

### Synchronizing Databases with ICMDBA

To synchronize the data of two Logger databases:

**Step 1** Start the ICMDBA tool from the Administration & Data Server program group.

**Step 2** Select a database from the main window and select **Synchronize** from the Data menu. The Synchronize window appears:

*Figure 20: Synchronize Window*
Step 3 Enter the server name and database for both source and target and select Synchronize.

Note: The ICMDBA synchronize process involves dropping the targeted side data and copying the data from the source. For example, if you are synchronizing side B data to side A data, the side B data will be replaced with the data stored in side A.

Cisco Unified Intelligent Contact Management Time Synchronization

This section describes the components that are involved in keeping the time-of-day clocks synchronized across all machines that comprise an Unified ICM system.

MDS

The Message Delivery Service (MDS) Synchronizer attempts to keep the system clocks of both sides of a duplexed system synchronized. The enabled Synchronizer is the time master, and the disabled Synchronizer is the time slave. The enabled Synchronizer supplies time messages every half-second to the synchronized application processes as well as to the disabled Synchronizer. To insulate applications against time discontinuities, the time supplied by the enabled Synchronizer is smoothed. If the system clock on the enabled side is changed, the enabled Synchronizer will supply time messages that appear to run 10% faster or slower (as needed) until the MDS time has converged with the system time.

The disabled Synchronizer receives time messages from the enabled Synchronizer every half second, and periodically compares the received time to the system time. In the event of a discrepancy greater than 100 milliseconds, the disabled Synchronizer uses system calls to run the system clock 10% faster or slower (as needed) until the discrepancy falls within tolerance. The net effect is that the systems clock on the disabled side smoothly tracks the MDS time, which in turn smoothly tracks the system clock on the enabled side.

MDS provides a "Set System Time" message API for setting the time. When MDS receives this message, the enabled Synchronizer sets the system time and the disabled Synchronizer does nothing (since it will track the clock of the enabled side). The "Set System Time" message should be sent by a synchronous process (on both sides of the system), since it cannot be determined which Synchronizer is the enabled one.

VRU PIM

The VRU PIM supports a mechanism for keeping the VRU time synchronized with Unified ICM time. The PIM periodically compares the time reported by the VRU to its own time, and sends a time adjustment message to the VRU if the times differ by more than about 15 seconds.

NAM/Customer ICM

In a Service Bureau installation, there can be multiple INCRP NICs running on the same machine (one per Customer ICM instance). However, only one of these NICs will be running on the ICM
instance that is in control of the system clock, and only this NIC is able to affect the time on
the CICM machine. This NIC will participate in time synchronization with the Network
Applications Managers (NAMs).

While initializing, each INCRP NIC will query MDS to determine whether it can control the
clock. Only one NIC on each machine will receive a positive response. This NIC will then
periodically (every few hours) send an unsolicited “Time Indication” message to one member
of each duplexed CIC pair. The time indication will include the NIC’s machine name and current
time.

Each duplexed CIC pair can be configured to be a "Time Server," a “Time Client," or "Passive." A CIC that is passive with regard to time synchronization forwards all received time indications
to the Routers for reporting purposes. A "Time Server" CIC additionally responds to each "Time
Indication" message from an INCRP NIC with a “Set Time Request” message containing its
own (MDS) time. (If the NIC and CIC reside on the same machine, as determined by the machine
name in the "Time Indication" message, the CIC will not send a "Set Time Request" – this
prevents the NAM and CICM from conflicting over control over the system clock.)

A "Time Client" CIC receives "Time Indication" messages and forwards them to the Routers
for reporting purposes. In addition, a time client CIC can also receive "Set Time Request"
messages. Upon receipt of a "Set Time Request" message, the CIC sends a "Set System Time"
message to the Routers, which in turn send a "Set System Time" message to MDS. Participation
of the Routers is required to ensure that the "Set System Time" message is delivered to MDS
on both sides of the system.

Similar processing occurs when an INCRP NIC receives a “Set Time Indication” from a (time
server) CIC: the NIC sends a "Set System Time" message to the Routers, and the Routers in
turn send a "Set System Time" message to MDS on both sides of the system. In addition, the
INCRP NIC forwards the “Set Time Indication” message to one member of each duplexed CIC
pair other than the one from which the original message was received. This serves to keep
multiple duplexed NAM pairs synchronized with each other.

CIC

The CIC can be configured with respect to time synchronization. A CIC configured to be a
“Time Server” responds to a "Time Indication" message from an INCRP NIC with a "Set Time
Request" message. A CIC configured to be a "Time Client" accepts "Set Time Request" messages
from INCRP NICs and sends a "Set System Time" message to the Router. All CICs forward
CICM time indications to the Routers for reporting.

The CIC Time Manager Type key in the registry is:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\instanceName\RouterA(B)\CIC\CurrentVersion\Configuration\CIC Time
Manager Type

To configure a CIC to be a Time Server, set the type to 2. To configure a CIC to be a Time
Client, set the type to 1. Setting the Type to 0 will only forward Time Indications to the Router.
Router

The Router attempts to keep the clocks of all controllers (NICs and PGs) synchronized with its own MDS time. It periodically queries each controller for its time. If the time discrepancy between the Router and controller is sufficiently large (15 seconds or more), the Router sends a time adjustment message to the controller instructing it to adjust its time by a delta value. The Router uses the round-trip delay of the query-response to account for transmission delay when computing the time adjustment.

Different controllers handle the time adjustment message in different ways. On a PG, OPC uses the MDS API to adjust the time of the (possibly duplexed) PG. A NIC ignores the time adjustment message, since adjusting the time on the Router machine could have unwanted feedback effects.

The Router records the time skew of all controllers and peripherals and can report these statistics via rttest.

In addition, the Router can optionally be configured via the Registry to designate one peripheral (usually an ACD) as a reference time source. When the Router receives a time update from the named peripheral, it invokes the MDS "Set System Time" API to set the Router time. This effectively synchronizes the Routers and all controllers to the reference time provided by the ACD.

Logger

The Router attempts to keep Loggers synchronized with its own Message Deliver Service (MDS) time. It periodically queries each Logger for its time. If the time discrepancy between the Router and Logger is 15 seconds or more, the Router sends a time adjustment message to the Logger instructing it to adjust its time by a delta value. The Logger then uses this delta value to adjust its time. The Router uses the round-trip delay of the query-response to account for transmission delay when computing the time adjustment.

ID Finder Tool

This section provides detailed information about the ID Finder tool.

About the ID Finder Tool

The ID Finder is a tool that allows configuration managers and administrators to find the various configuration IDs of the following Unified ICM components:

- Agent
- Label
- NIC
The ID Finder tool helps you easily search for the IDs for particular Unified ICM components. You can identify the component ID, record type, and the name of the component from the search results by entering an ID or range of IDs.

Most of the Unified ICM configuration tools do not show component IDs in the user interface; you need to look for the component IDs while setup or during configuration.

Also, for Unified SCCE the ID Finder tool can be used for identifying the component IDs.

The user interface of this tool is shown in the following figure.

Figure 21: The ICM ID Finder Tool

Using the ID Finder Tool

The ID Finder tool is used mainly in the following three cases:
During Unified ICM setup, the peripheral ID is required to setup a PG. The ID Finder tool enables you to access the peripheral IDs.

The Unified ICM logs usually list the component IDs. During troubleshooting, the ID Finder tool can be used to look for the object names by component IDs.

In Unified SCCE, you do not see the component IDs. The ID Finder tool helps you to get the component IDs whenever necessary.

How to Access the ID Finder Tool

The ID Finder tool is available as an executable file, idfinder.exe, starting in Unified ICM Release 4.6(2).

You can access this tool from all Unified ICM Administration & Data Servers from the following path: icm\bin\idfinder.exe.

Starting in Release 7.1(1), the ID Finder tool is enhanced to provide the Unified ICM application path of the component ID.

How to Use the ID Finder Tool

To use the ID Finder tool, perform the following steps:

**Step 1** Access ICM > Bin.

**Step 2** Double-click idfinder.exe. The ID Finder window displays.

**Step 3** Enter the ID range (for example, 5000-6000) in the ID Number.

**Step 4** Select the ID Type (for example, Agent, Label) from the list, as shown in the figure below:

![Figure 22: ICM ID Finder Tool: ID Types](image)

**Step 5** Select Search Now to get the results.
Modifying the Skill Groups Per Agent Limit

Unified ICM and Unified CCE impose a default limit on the number of skill groups that you can assign to a single agent. Once this limit is reached, additional skill groups cannot be assigned. The default limit is specified in the Cisco Unified Contact Center Enterprise 8.x Solution Reference Network Design (SRND). The limit considers the total of both skill groups and sub-skill groups.

If desired, you can use the ConfigLimit Tool to specify your own limit on the number of skill groups that can be assigned to an agent. For optimum performance, you can specify a limit far lower than the system default (refer to the Cisco Unified Contact Center Enterprise 8.x Solution Reference Network Design (SRND) for performance considerations in choosing a skill groups per agent limit).

Warning: Setting a default value for skill groups per agent that is higher than the system default can adversely affect system performance. Cisco will not support configurations that exceed the default value.

Caution: The ConfigLimit tool is a command-line tool utility from the bin directory of all Unified ICM/CCE Administration & Data Servers. Access is limited to users with privileges for the Setup or Config Groups in Active Directory for the chosen customer instance. (Refer to the Outbound Option Guide for Cisco Unified Contact Center Enterprise & Hosted for detailed information about the ConfigLimit tool.)

Using the ConfigLimit Tool

To change the skill groups per agent limit in configlimit.exe:

**Step 1**
Launch a command line window on any Administration Client or Administration & Data Server.

**Step 2**
Enter `configlimit`.

**Step 3**
 Optionally, enter `cl /show` to view the existing limit.

**Step 4**
To change the limit, enter `cl /id 1 value/<new_value> /update`

For example, to change the skill groups per agent limit to 5, enter the following text: `cl /id 1 value/5 /update`

**Step 5**
Press Enter.
### Additional Requirements

#### Lowering the Limit

If you have modified the skill groups per agent limit to be lower than the system default, no additional changes are necessary. The new, lower limit will be enforced immediately. Note that the new limit will *not* impact agents whose existing skill group membership exceeds the new limit until the next attempt to add a new skill group for those agents. At that time the new limit will be enforced, preventing you from adding additional skill groups.

#### Exceeding the Default Limit

If you have modified the skill groups per agent limit to be higher than the system default (in spite of the Warning given above), certain deployments will require additional changes (listed in the following sections) to your system to use the new limit and will allow you to add additional skill groups.

**Note:** If you exceed the default limit and are using CTI OS, **do not exceed** a maximum of 99 skill groups.

### IPCC Gateway PG

For IPCC Gateway deployments, modify the following registry keys on your IPCC Gateway PGs to include the new value. A change to the registry will require that the PG service be restarted.

**IPCC Enterprise Gateway PIM (Cisco Unified Contact Center Enterprise parent)**

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\< customer_instance >\PG{n}[A|B]\PG\CurrentVersion\PIMS\pim(m)\ACMIData\Config\MaxSkills
```

**IPCC Express Gateway PIM (Cisco Unified Contact Center Express parent)**

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\< customer_instance >\PG{n}[A|B]\PG\CurrentVersion\PIMS\pim(n)\ACMIData\Config\MaxSkills
```

### ERI PG

For ERI deployments, modify the following registry key on your ERI PGs to include the new value. A change to the registry will require that the PG service be restarted.

**ER Service PIM**

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\< customer_instance >\PG{n}[A|B]\PG\CurrentVersion\PIMS\pim(n)\ERSData\Config\MaxSkills
```
Chapter 6

Partitioning Overview

As of Unified ICM Release 8.0(1), Partitioning is no longer supported except on systems that already have Partitioning installed.

For example, if you have Partitioning installed on your Unified ICM Release 7.5(1) system, you can upgrade from 7.5(1) to 8.0(1) and retain your Partitioning.

However, you cannot newly implement Partitioning on a Unified ICM Release 8.0(1) system.

See Also

Index

accessing ID Finder tool....77

administration
  built-in....66
  optional....66

Administration & Data Server
  Administration Tools folder....11
  overview....8
  Unified CCE Tools folder....9

Administration Clients, receiving real-time data....30

agent log in flexibility....17, 18
back-up strategies....70
call detail data....36
call routing, Network Interface Controllers....27

Central Controller
  Administration & Data Server....12
  Network Interface Controllers....27

central database
  monitoring the size of....62
  sizing and usage....46
  storage capabilities....46
changes....13

ConfigLimit tool, using....78
configuration checks....66
configuration data....13, 35, 36, 38
Configuration Management Service (CMS)....39
configuring
  CIC....74
  server....56

Create function
  with configured components....49
  without configured components....50
creating

new data device....50, 51

Unified ICME database with configured components....49
Unified ICME database without configured components....50

CTI port, DN....16, 19
database administration
  fault tolerance....15
  overview....7

Database Properties function....53

Database Retriever dialog, querying system's configuration information....60
databases
  adding space....63
  administration overview....45
  backing up....70
  central....36
  central and local....12
  comparing....71
  configuration checks....66
  creating....38
  disk failure....27
  full indicator....61
  integrity checks....66
  local (awdb)....38
  networking support....68
  overview....33
  recovery....26
  resynchronizing....71
  service bureau....35
  sizing and creation....37
  synchronizing from the Command window....72
  synchronizing with ICMDBA....72
  temporary....40
  tools....34
  updates and changes....38
Database Sizing Estimator applet
  estimating size of database....59
  starting....58
  using to estimate database size....58
data integrity checks....66
data types....35
DBCC CHECKDB procedure....66
Delete function....51
deleting databases....51
deployments
  Large HDS....41
  Small to Medium HDS....40
domain adherence integrity check....68
duplexed
  Central Controller....19
databases....37
enterprise integrity check....67
estimating databases....59
events
  data storage....36
Expand function....52
expanding database on storage device....52
exporting data....54
failures
  disk....27
  software....27
  system....26
fault tolerance
  approaches....16
  architecture of Unified ICM system....7
database....25
database administration....15
  integrated deployments....31
five-minute data....36
HDS machine, setting up Administration & Data Server with HDS....60
historical data....35
  interval....36
  retention....46
Historical Data Server
  about historical data....30
  architecture....40
  Large deployments....41
  Small to Medium deployments....40
ICMDBA tool
  accessing functions....49
  Add Device window....50, 51
  Configure window....56
  configuring server....56
  Create function with configured components....49
  Create function without configured components....50
Database Properties function....53
Delete function....51
Expand Database window....52
Expand function....52
Import/Export functions....54
  importing and exporting data....54
  main window....48
  Recreate Database window....53
  Recreate function....53
  starting....48
  Synchronize function....55
  Synchronize window....55
  table groups....49
  Table Properties function....54
  using to start or stop a server....47
  viewing table properties....49
ICM ID Finder Tool
  about....75
  ID Finder Tool
    accessing....77
using....76
importing data....54
Initialize Local Database tool....34
initializing local database....63
limit, skill groups....78
local agent, defined....16, 18
Lock Administration....13
locking data....42
locks
   Master....43
   releasing....43
Logger
   time synchronization....75
Logger events, viewing....68
MDS Synchronizer....73
Message Delivery Service (MDS)....73
mirrored disks....70
Mobile Agent overview....16, 18
NAM, service bureau installations....73
names integrity check....68
nulls integrity check....67
Open Peripheral Controller....28
partitioning, Unified ICME feature, about....81
performing backups....71
peripheral gateways, duplexed....28
preventing users from changing data simultaneously....42
purging data
   automatic, database full....62
   emergency, deleting oldest historical data....62
RAID....70
real-time
   administration....30
   data....38
real-time data....35, 38
recovery
   CallRouter....24
   database....26
   Logger....25
   recreation function....53
   recreating a database....53
   releasing locks....43
   Remote Agent, defined....16, 18
   restarting Unified ICM processes after an exception....69
   Router, time synchronization....75
   routes and numbers integrity check....67
   script data....35
   scripts, routing....36, 38
   scripts integrity check....67
   setting up HDS machine
      when instance is created, already added....61
      when instance is created, not added....61
   simplex configurations....31
   sizing
      databases....37
      databases using the Database Sizing Estimator applet....58
   skill groups, limit....78
   snapshot data....35
   SQL Monitor....70
   SQL Server
      for multiple customers....35
   starting
      Database Sizing Estimator application....58
      ICMDBA tool....48
   Synchronize function....55
   synchronizers
      geographic....21
      role....22
      state transfer....23
   synchronizing databases....55
   table groups....49
Table Properties function....54
tables, comparing....71
targets integrity check....67
TEMPDB database....34
time synchronization, Unified ICME....73
tools
  Administration....8
  Administration Tools folder....11
  ConfigLimit....78
  Database Retriever dialog....60
  Database Sizing Estimator web applet....58
  ICMDBA....47
  ICM ID Finder....75
  Unified CCE Tools folder....9
transaction logs....70
upgrading systems with SQL 2000....37
using
  ID Finder tool....76, 77
viewing
  database properties....53
  table properties....49, 54
VRU PIM time synchronization....73