Cisco Unified Web and E-Mail Interaction Manager System Administration Guide
For Unified Contact Center Enterprise and Hosted and Unified ICM

Release 4.2(1)
August 2007

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

Preface .................................................................................................................................................5
  About this guide ................................................................. 6
  Document conventions ....................................................... 6
  Other learning resources .................................................... 6
    Online help ........................................................................ 7
    Documentation ............................................................... 7

Chapter 1: Setting up an integrated installation ...................................................................................8
  Relationship between objects in Unified CCE and Cisco Interaction Manager ......................... 9
  Designing your installation .................................................. 9
  Preparing Unified CCE for the integration .................................... 10
    Obtaining Cisco Interaction Manager licenses ...................................... 10
    Installing Unified CCE .................................................................. 10
    Configuring Unified CCE ............................................................. 10
  Preparing Unified SCCE for the integration ...................................... 31
    Obtaining Cisco Interaction Manager licenses ...................................... 31
    Installing Unified SCCE .................................................................. 31
    Configuring Unified SCCE ............................................................. 31
  Installing Cisco Interaction Manager and the integration ................................................. 46
  Configuring objects in Cisco Interaction Manager ................................................................. 46
    Verifying mapping of objects in the Administration Console .............................. 47
    Setting up knowledge base articles for Unified EIM ..................................... 50
    Setting up business objects in the Administration Console .......................... 52
    Setting up services in the System Console ........................................... 55
    Setting up web links for chat ...................................................... 62
    Related documentation ............................................................ 63

Chapter 2: Configuring web server ...................................................................................................64
  Configuring Internet Information Services ................................................................. 65
Chapter 3: Managing application servers ................................................................. 69

- Configuring WebLogic ................................................................. 70
- Routine maintenance tasks ............................................................. 71
  - Creating backup copies ............................................................... 71
  - Archiving .................................................................................. 72
  - Applying Microsoft security patches and service packs..................... 72

Chapter 4: Managing databases ............................................................................ 73

- Best practices for configuring databases .............................................. 74
- Installation and settings ........................................................................ 74
- Optimal configuration settings ............................................................ 74
- Configuring anti-virus protection ......................................................... 75
- Routine maintenance tasks ................................................................. 75
  - Rebuilding indexes ....................................................................... 75
  - Optimizing database file space ...................................................... 75
  - Performing disk defragmentation .................................................... 75
  - Creating backup copies .................................................................. 75
  - Archiving .................................................................................... 76
  - Applying Microsoft security patches and service packs .................... 76

Chapter 5: Managing Windows servers ............................................................... 77

- Best practices for configuring Windows servers ................................... 78
  - Allocating adequate virtual memory ............................................... 78
  - Setting up disk space ...................................................................... 78
  - Configuring anti-virus protection .................................................... 78
- Routine maintenance tasks ................................................................. 78
  - Monitoring disk space .................................................................... 78
  - Applying Microsoft security patches and service packs .................... 78
- Performance tuning considerations ...................................................... 79
  - Peak concurrent usage ................................................................... 79
  - Email volume ............................................................................... 79
  - Server configuration ....................................................................... 79
  - Security requirements ..................................................................... 79
Preface

- About this guide
- Document conventions
- Other learning resources
Welcome to Cisco® Interaction Manager™, multichannel interaction software used by businesses all over the world to build and sustain customer relationships. A unified suite of the industry’s best applications for web and email interaction management, it is the backbone of many innovative contact center and customer service helpdesk organizations.

Cisco Interaction Manager includes a common platform and one or both of the following applications:

- Cisco Unified Web Interaction Manager (Unified WIM)
- Cisco Unified E-Mail Interaction Manager (Unified EIM)

**About this guide**

*Cisco Unified Web and E-Mail Interaction Manager System Administration Guide* discusses best practices for maintaining your Cisco Interaction Manager installation. This guide is intended for system and database administrators. It will help you keep the installation in good health and to fine tune it to improve its performance.

This guide is for installations that are integrated with Cisco Unified Contact Center Enterprise (Unified CCE) or Unified System Contact Center Enterprise (Unified SCCE).

---

**Important:** In this release, Unified WIM is not integrated with Unified CCE.

---

**Document conventions**

This guide uses the following typographical conventions.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Italic</strong></td>
<td>Emphasis. Or the title of a published document.</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Labels of items on the user interface, such as buttons, boxes, and lists. Or text that must be typed by the user.</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>The name of a file or folder, a database table column or value, or a command.</td>
</tr>
<tr>
<td><strong>Variable</strong></td>
<td>User-specific text; varies from one user or installation to another.</td>
</tr>
</tbody>
</table>

**Other learning resources**

Various learning tools are available within the product, as well as on the product CD and our web site. You can also request formal end-user or technical training.
Online help

The product includes topic-based as well as context-sensitive help.

<table>
<thead>
<tr>
<th>Use</th>
<th>To view</th>
</tr>
</thead>
<tbody>
<tr>
<td>📚 Help button</td>
<td>Topics in Cisco Unified Web and E-Mail Interaction Manager Help; the Help button appears in the console toolbar on every screen.</td>
</tr>
<tr>
<td>F1 keypad button</td>
<td>Context-sensitive information about the item selected on the screen.</td>
</tr>
</tbody>
</table>

Online help options

Documentation

- The latest versions of all Cisco documentation can be found online at [http://www.cisco.com](http://www.cisco.com)
Setting up an integrated installation

- Designing your installation
- Preparing Unified CCE for the integration
- Preparing Unified SCCE for the integration
- Installing Cisco Interaction Manager and the integration
- Configuring objects in Cisco Interaction Manager
This chapter provides an overview of the process of setting up an integrated Cisco Interaction Manager–Unified CCE system. It includes a note about the relationship between objects in Unified CCE and Cisco Interaction Manager.

**Relationship between objects in Unified CCE and Cisco Interaction Manager**

This section provides a brief introduction to the relationship between objects that are used in both systems.

The mapping between objects can be set up in either system. You can map objects by running the Cisco Interaction Manager integration wizard for each partition and department. Or you can create new objects in Cisco Interaction Manager and map them to objects in Unified CCE from the Cisco Interaction Manager Administration Console. Properties of mapped objects are typically set up in Unified CCE, while permissions are managed through Cisco Interaction Manager.

The following table provides a high-level view of the relationship between various objects.

<table>
<thead>
<tr>
<th>Unified CCE object</th>
<th>Mapped in Cisco Interaction Manager to</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>User</td>
<td>› An agent belongs to a peripheral.</td>
</tr>
<tr>
<td>Supervisor</td>
<td></td>
<td>› A peripheral belongs to an agent peripheral gateway (PG).</td>
</tr>
<tr>
<td>Administrator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skill group</td>
<td>User group</td>
<td>› A skill group belongs to a peripheral.</td>
</tr>
<tr>
<td>Media routing domain (MRD)</td>
<td>Queue</td>
<td>› A peripheral belongs to an agent PG.</td>
</tr>
<tr>
<td>Script selector</td>
<td>Queue</td>
<td>› Multiple queues can belong to a single MRD.</td>
</tr>
</tbody>
</table>

**Note:** For chat, you will need to set up queues in Cisco Interaction Manager as the routing of chat interactions is not integrated with Unified CCE in this release.

**Designing your installation**

See *Cisco Unified Web and E-Mail Interaction Manager Solutions Reference Network Design Guide* (for Unified CCE) to evaluate available deployment models and design your installation.
Preparing Unified CCE for the integration

Obtaining Cisco Interaction Manager licenses

To order licenses for your Cisco Interaction Manager deployment, contact the Cisco License team. You will need the licenses to set up the integrated system.

Installing Unified CCE

Ensure that Unified CCE is installed and available for use. See the following documents for help with installing and configuring the system:

- Getting Started with Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Enterprise Installation Guide

Configuring Unified CCE

In this section, we describe the process of preparing Unified CCE for the integration with Unified WIM and Unified EIM. It involves configuring the following objects (in the order specified):

1. Application instance
2. Media classes
3. Media routing domains (MRD)
4. Network voice response unit (VRU)
5. Call type
6. Script selector
7. Media routing peripheral gateway (MR PG)
8. Agent desk settings
9. Agent peripheral gateway (Agent PG)
10. Application path
11. Agents
12. Services
13. Skill groups
14. Scripts
Configuring application instance

An application instance refers to a Cisco Interaction Manager deployment that is integrated with Unified CCE. It is required for downloading configuration objects from Unified CCE and mapping these to Cisco Interaction Manager.

Configure a single application instance for Unified WIM and Unified EIM.

To configure an application instance:

1. Go to Start > All Programs > ICM Admin Workstation > Configuration Manager.
2. In the Configuration Manager window, browse to Tools > List Tools > Application Instance List.
3. Double-click Application Instance List.
4. In the Application Instance List window, in the Select filter data section, click Retrieve. Then, in the Application Instance section, click Add.
   A new entry is created in the Application Instance section and the Attributes tab becomes editable.
5. On the Attributes tab, provide the following details:
   - **Name**: Provide a name for the application instance.
   - **Application key**: Click the Change Application Key button and provide a unique value for the key.
   - **Application type**: Set it to <Other>.
   - **Permission level**: Set it to Read only.

Click Save.

Configure the application instance
**Configuring media classes**

A media class is required for creating MRDs. It helps categorize the MRDs based on media type, for example, email. Create a media class for email. The media class for voice already exists.

**To configure a media class:**

1. Go to **Start > All Programs > ICM Admin Workstation > Configuration Manager.**
2. In the Configuration Manager window, browse to **Tools > List Tools > Media Class List.**
3. Double-click **Media Class List.**
4. In the Media Class List window, in the Select filter data section, click **Retrieve.** Then, in the Media Class section, click **Add.**

   A new entry is created in the Media Class section and the Attributes tab becomes editable.

5. On the Attributes tab, provide the following details:
   - **Name:** Provide a name for the media class.
   - In the Task section, set the following:
     - **Life:** 300 seconds
     - **Start timeout:** 30 seconds
     - **Max Duration:** 28800 seconds

   Click Save.
Configuring media routing domains

A media routing domain is created in Unified CCE for mapping to queues in Cisco Interaction Manager. For the email media class, configure one or more email media routing domains.

**To configure a media routing domain:**

1. Go to Start > All Programs > ICM Admin Workstation > Configuration Manager.
2. In the Configuration Manager window, browse to Tools > List Tools > Media Routing Domain List.
4. In the Media Routing Domain List window, in the Select filter data section, click Retrieve. Then, in the Media Routing Domain section, click Add.

   A new entry is created and the Attributes tab becomes editable.

5. On the Attributes tab, provide the following details:
   - **Name:** Provide a name for the media routing domain.
   - **Media class:** Select a media class created for Cisco Unified Web and E-Mail Interaction Manager.

   In the Calls in Queue section, set the following:
   - **Max:** Specify a value. If no value is provided, a default value of 5000 is used for Cisco Interaction Manager.

   Click Save.

![Configure media routing domains](image)

Configuring network voice response unit

Network voice response unit (VRU) is required for supporting incoming voice calls to Unified CCE.
To configure a network voice response unit (VRU):

1. Go to Start > All Programs > ICM Admin Workstation > Configuration Manager.
2. In the Configuration Manager window, browse to Tools > Explorer Tools > Network VRU Explorer.
4. In the Network VRU window, in the Select filter data section, click Retrieve. Then, click [1] Add Network VRU.
   A new entry is created and a new set of tabs appear.
5. On the Network VRU tab, provide the following details:
   - **Name**: Provide a name for the network VRU.
   - **Type**: Set it to Type 2.
   Click Save.

![Configure network VRU](image)

6. Click Add Label.
   The Label tab appears.
7. On the Label tab, provide the following details:
   - **Routing client**: From the dropdown list, select a routing client.
   - **Label**: Provide a name for the label.
   Click Save.

**Configuring call types**

A call type is required to categorize a dialed number (for voice) or script selector (for email). Call types are used in configuring ICM routing scripts.
To configure a call type:

1. Go to Start > All Programs > ICM Admin Workstation > Configuration Manager.
2. In the Configuration Manager window, browse to Tools > List Tools > Call Type List.
3. Double-click Call Type List.
4. In the Call Type List window, in the Select filter data section, click Retrieve. Then, in the Call Type section, click Add.
   A new entry is created and the Attributes tab becomes editable.
5. On the Attributes tab, in the Name field, provide a name for the call type. Click Save.

Provide the name of the call type

Configuring script selectors

A script selector is a keyword that identifies the ICM routing script for an activity request from Cisco Interaction Manager to Unified CCE. Script selectors are used in the ICM routing scripts as part of the Dialed Number node.

To configure a script selector:

1. Go to Start > All Programs > ICM Admin Workstation > Configuration Manager.
2. In the Configuration Manager window, browse to Tools > List Tools > Dialed Number/ Script Selector List.
3. Double-click Dialed Number/ Script Selector List.
4. In the Dialed Number/ Script Selector List window, in the Select filter data section, click Retrieve. Then, in the Dialed Number/ Script Selector section, click Add.
   A new entry is created and the Attributes tab becomes editable.
5. On the Attributes tab, provide the following details:
- **Routing client**: From the dropdown list, select a routing client.
- **Media routing domain**: From the dropdown list, select the MRD configured for Unified WIM and Unified EIM (page 13).
- **Name**: Provide a name for the script selector.

Click Save.

![Configure script selector](image)

**Configuring media routing peripheral gateways**

An MR PG handles new activity routing requests initiated by Cisco Interaction Manager, over the connection established by the embedded MR PIM (side A or side B).

---

**Important**: Before configuring an MR PG, make sure an MR PIM is installed. For installing MR PIM, see the Unified CCE installation guide.

---

**To configure a media routing peripheral gateway (MR PG):**

1. Go to **Start > All Programs > ICM Admin Workstation > Configuration Manager**.
2. In the Configuration Manager window, browse to **Tools > Explorer Tools > PG Explorer**.
3. Double-click **PG Explorer**.
4. In the PG Explorer window, in the Select filter data section, click **Retrieve**. Then, click **[1] Add PG**.
5. On the Logical Controller tab, provide the following details:
   - **Name**: Provide a name for the media routing peripheral gateway.
   - **Client type**: Set it to MR PG.

A new set of tabs appear.

7. On the Peripheral tab, select the **Enable Post Routing** option.
8. On the Advanced tab, in the **Network VRU** field, from the dropdown list, select the network VRU configured for Unified WIM and Unified EIM (page 13).

Select a network VRU

9. On the Routing client tab, provide the following details:
   - **Name**: Provide a name for the routing client.
   - **Default media routing domain**: From the dropdown list, select the MRD configured for Unified WIM and Unified EIM (page 13).
   - **Default call type**: From the dropdown list, select the call type configured for Unified WIM and Unified EIM (page 14).

Click Save.
10. On the Default route tab, in the **Media Routing Domain** field, from the dropdown list, select an MRD configured for Unified WIM and Unified EIM (page 13).

![](image)

**Select an MRD**

### Configuring agent desk settings

Agent desk settings are a common set of properties for a group of agents working on voice call requests.

**To configure agent desk settings:**

1. Go to **Start > All Programs > ICM Admin Workstation > Configuration Manager**.
2. In the Configuration Manager window, browse to **Tools > List Tools > Agent Desk Settings List**.
3. Double-click **Agent Desk Settings List**.
4. In the Agent Desk Settings List window, in the Select filter data section, click **Retrieve**. Then, in the Agent Desk Settings section, click **Add**.

   A new entry is created and the Attributes tab becomes editable.

5. On the Attributes tab, in the **Name** field, provide a name for the agent desk setting group. Click **Save**.
Configuring agent peripheral gateway

An Agent PG is required for creating of one or more peripherals that manage agent distribution within Unified CCE. Configure an agent peripheral gateway (PG) using the Configuration Manager and then install it on the appropriate machine.

To configure an agent peripheral gateway:

1. Go to Start > All Programs > ICM Admin Workstation > Configuration Manager.
2. In the Configuration Manager window, browse to Tools > Explorer Tools > PG Explorer.
3. Double-click PG Explorer.
4. In the PG Explorer window, in the Select filter data section, click Retrieve. Then, click [1] Add PG.
5. On the Logical Controller tab, provide the following details:
   - **Name**: Provide a name for the agent peripheral gateway.
   - **Client type**: Set it to CallManager/SoftACD.
   - **Primary CTI address**: Provide the address of the primary CTI server in the format `IP_Address:Port_Number`. 

Provide the name of the agent desk settings group
Secondary CTI address: Provide the address of the secondary CTI server in the format `IP_Address:Port_Number`. This is optional.


   A new set of tabs appear.

7. On the Peripheral tab, in the Default desk settings field, from the dropdown list, select the agent desk settings configured for Unified WIM and Unified EIM (page 19).

8. On the Agent Distribution tab, do the following:
   a. Click New.
b. Select the **Enable agent reporting** option.

c. Select the **Agent event detail** option.

d. In the Currently Selected Site section, set the following:
   - **Distributor site name**: Provide the host name of the machine where distributor is installed.
   - **Enable**: Select the option.

Click Save.

---

### Configuring application path

An application path is required to open a communication channel with a CTI server, associated with an Agent PG, for agent and task status reporting. For each agent PG create an application path, which Unified WIM and Unified EIM will use to connect to the agent PG.

> **Important:** For configuring an application path you need to login using an account with superuser privileges.

#### To configure an application path:

1. Go to **Start > All Programs > ICM Admin Workstation > Configuration Manager**.
2. In the Configuration Manager window, browse to **Tools > List Tools > Application Path List**.
3. Double-click **Application Path List**.
4. In the Application Path List window, in the Select filter data section, click **Retrieve**. Then, in the Application Path section, click **Add**.
   
   A new entry is created and the Attributes tab becomes editable.
5. On the Attributes tab, provide the following details:
- **Application Instance**: From the dropdown list, select an application instance configured for Unified WIM and Unified EIM (page 11).
- **Peripheral Gateway**: From the dropdown list, select an agent peripheral gateway configured for Unified WIM and Unified EIM (page 20).
- **Name**: This field is auto-populated.

In the Application Path Members section, click the **Add** button and set the following:
- **Peripheral**: From the dropdown list, select the agent peripheral configured for Unified WIM and Unified EIM (page 20).
- **Media routing domain**: From the dropdown list, select an MRD configured for Unified WIM and Unified EIM (page 13).

Click **Save**.

![](Configure_application_path.png)

### Configuring agents

An agent is created in Unified CCE for mapping to users in Cisco Interaction Manager.

**To configure an agent:**

1. Go to **Start > All Programs > ICM Admin Workstation > Configuration Manager**.
2. In the Configuration Manager window, browse to **Tools > Explorer Tools > Agent Explorer**.
3. Double-click **Agent Explorer**.
4. In the Agent Explorer window, in the Select filter data section, click **Retrieve**. Then, click **Add Agent** button.
   A new entry is created and a new set of tabs appear.
5. On the Agent tab, provide the following details:
   - **First name**: Provide the first name.
Configure an agent

Configuring services

A service is defined for a peripheral to describe the category of requests being processed by skill groups that belong to the peripheral. For example, billing, inventory, etc. A service is required for creating skill groups.

**To configure a service:**

1. Go to Start > All Programs > ICM Admin Workstation > Configuration Manager.
2. In the Configuration Manager window, browse to Tools > Explorer Tools > Service Explorer.
3. Double-click Service Explorer.
4. In the Service Explorer window, in the Select filter data section, click Retrieve. Then, click Add Service button.
   
   A new entry is created and a new set of tabs appear.
5. On the Service tab, provide the following details:
   - **Media routing domain:** From the dropdown list, select an MRD configured for Unified WIM and Unified EIM (page 13).
   - **Peripheral number:** Provide a unique peripheral number.
   - **Name:** Provide a name for the service.
Configuring skill groups

A skill group is created in Unified CCE for mapping to user groups in Cisco Interaction Manager. You can create two types of skill groups:

- **Cisco Interaction Manager picks the agent (Non-IPTA):** For a Non-IPTA skill group, the skill group members (agents) are administered and managed in Cisco Interaction Manager. A Non-IPTA skill group is created for email routing in cases where a label is returned by Unified CCE to Cisco Interaction Manager. When a label is returned, Cisco Interaction Manager load balances the email activity to a group of agents defined in the user group (that maps to the Non-IPTA skill group) identified by the suffix of the label.

- **ICM-picks-the-agent (IPTA):** For an IPTA skill group, the skill group members (agents) are administered and managed in Unified CCE. An IPTA skill group (with associated skill group members) is used in ICM scripts to facilitate email routing through Unified CCE to the skill group.

**To configure an IPTA skill group:**

1. Go to Start > All Programs > ICM Admin Workstation > Configuration Manager.
2. In the Configuration Manager window, browse to Tools > Explorer Tools > Skill Group Explorer.
   
   A new entry is created and a new set of tabs appear.
5. On the Skill Group tab, provide the following details:
   
   - **Media routing domain:** From the dropdown list, select an MRD configured for Unified WIM and Unified EIM (page 13).
   - **Peripheral number:** Provide a unique peripheral number.
- **Peripheral name**: Provide a name for the skill group.
- **Name**: This field is auto-populated.
- **ICM picks the agent**: Select the option.

Configure the properties of an IPTA skill group

6. On the Skill Group Members tab, do the following:
   a. Click the **Add** button.
   b. From the Add Skill Group Member window, select the agents to be added in the skill group. Click **OK**.

Select members for the skill group

7. Click the **Add Route** button.
   A new tab appears.

8. On the Route tab, in the **Name** field provide the name for the route and click **Save**.
To configure a non-IPTA skill group:

1. Go to Start > All Programs > ICM Admin Workstation > Configuration Manager.
2. In the Configuration Manager window, browse to Tools > Explorer Tools > Skill Group Explorer.
   A new entry is created and a new set of tabs appear.
5. On the Skill Group tab, provide the following details:
   - **Media Routing Domain**: From the dropdown list, select an MRD configured for Unified WIM and Unified EIM (page 13).
   - **Peripheral Name**: Provide a name for the skill group.
   - **Name**: This field is auto-populated.
   - **ICM picks the agent**: Clear the option.

Click Save.
Configure a non-IPTA skill group

6. Click the **Add Route** button.

A new tab appears.

7. On the Route tab, in the **Name** field provide the name for the route and click **Save**.
Configuring scripts

An ICM routing script determines the path and target object for an activity routed from Cisco Interaction Manager to Unified CCE. You need to configure scripts for email routing.

To configure a script:
1. Go to Start > All Programs > ICM Admin Workstation > Script Editor.
2. In the Script Editor window, click the New button.
3. In the Create A New Script window, select the Routing script option.

A new script editor opens. The Star node is added by default to the script editor.

4. On the Routing tab, click the Dialed Number button, and click in the script editor. The Dialed Number (DN) node is added to the script editor.
5. Double-click the DN node to open the DN Properties window.
6. In the DN Properties window, on the Dialed Number node, from the list of available script selectors select a script selector and click the Add button. Click OK.

7. On the Targets tab, click the Skill Group button, and click in the script editor. The Skill Group node is added to the script editor.
8. Double-click the Skill Group node to open the Skill Group Properties window.
9. In the Skill Group Properties window, on the Routing Target tab, in the Skill Group column, select an IPTA skill group.

![Skill Group Properties window](image)

Select an IPTA skill group

10. Next, on the Targets tab, click the **Label** button, and click in the script editor. The Label node is added to the script editor.

11. Double-click the Label node to open the Label window.

12. In the Label window, on the Label tab, set the following:
   a. Select the label type as **Configured**.
   b. From the available labels select a label and click the **Add** button. Click OK.

![Label Properties window](image)

Select the label type and a label

13. Next, on the General tab click the **Line Connector** button, and configure the success and error paths for each node. This creates the routing path of the script.

14. Click the **Validate** button to check if the script is created properly. If there are any errors, fix them.
15. Click the **Save** button to save the script.

---

**Preparing Unified SCCE for the integration**

**Obtaining Cisco Interaction Manager licenses**

- To order licenses for your Cisco Interaction Manager deployment, contact the Cisco License team. You will need the licenses to set up the integrated system.

**Installing Unified SCCE**

- Ensure that Unified SCCE is installed and available for use. See the following document for help with installing and configuring the system:

**Configuring Unified SCCE**

In this section, we describe the process of preparing Unified SCCE for the integration with Unified WIM and Unified EIM. It involves configuring the following objects (in the order specified):

1. All-in-one server
2. Multichannel controller server
3. Agent desk settings
4. Agent teams
Configuring all-in-one servers

To configure an all-in-one server:

1. Type the URL `https://unified_SCCE_Server_Name/uiroot/default/ipccAdmin/loginAdmin.jsp` in your browser.

2. In the Login window, type the Administrator desktop login name and password. Click the Login button.

3. In the Cisco IPCC Enterprise Web Administration window, browse to IPCC Enterprise > System Management > Machine Management > Machines.

4. In the Machines section, click the machine name of the all-in-one server. Alternately, click Create to add a new all-in-one server.

5. In the Describe the IPCC Machine in your deployment window, view or edit the hostname and role of the machine. Click Next.
6. In the Edit IPCC Network settings window, view or edit the network settings of the machine. Click Next.

7. In the Edit CallManager Connectivity Settings window, view or edit the call manager connectivity settings. For details on how to create a CallManager JTAPI User ID, see http://www.cisco.com/univercd/cc/td/doc/product/icm/ipce70d/ipccor7/ipce70ic.pdf. Click Next.
View the call manager connectivity settings

8. In the IVR connectivity settings window, view or edit the IVR connectivity settings. Click Next.

View the IVR connectivity settings

9. In the Database settings window, view or edit the database settings. Click Next.
View the database settings

10. Click the **Finish** button to save the settings for the machine.

**Configuring multichannel controller server**

**To configure a multichannel controller server:**

1. Type the URL `https://unified_SCCE_Server_Name/uiroot/default/ipccAdmin/loginAdmin.jsp` in your browser.

2. In the Login window, type the Administrator desktop login name and password. Click the **Login** button.

3. In the Cisco IPCC Enterprise Web Administration window, browse to **IPCC Enterprise > System Management > Machine Management > Machines.**
4. In the Machines section, click the machine name of the multichannel controller server. Alternately, click Create to add a multichannel controller server.

5. In the Describe the IPCC Machine in your deployment window, view or edit the hostname and role of the machine. Click Next.

View the hostname and role of the machine

6. In the Edit IPCC Network settings window, view or edit the network settings of the machine. Click Next.
7. Click the Finish button to save the settings for the machine.

Configuring agent desk settings

To configure an agent desk setting:

1. Type the URL https://Unified_SCCE_Server_Name/uiroot/default/ipccAdmin/loginAdmin.jsp in your browser.
2. In the Login window, type the Administrator desktop login name and password. Click the Login button.
3. In the Cisco IPCC Enterprise Web Administration window, browse to IPCC Enterprise > Agent Management > Desk Settings.
4. In the Desk Settings section, click the **DefaultDesktopSettings** link to view the desk settings that apply to all configured agents. Alternately, create a new desk setting by clicking **Create**.

View desk settings details

**Configuring agent teams**

**To configure an agent team:**

1. Type the URL `https://unified_SCCE_Server_Name/uiroot/default/ipccAdmin/loginAdmin.jsp` in your browser.

2. In the Login window, type the Administrator desktop login name and password. Click the **Login** button.

3. In the Cisco IPCC Enterprise Web Administration window, browse to **IPCC Enterprise > Agent Management > Teams.**
To configure an agent:

1. Type the URL `https://unified_SCCE_Server_Name/uiroot/default/ipccAdmin/loginAdmin.jsp` in your browser.

2. In the Login window, type the Administrator desktop login name and password. Click the **Login** button.

3. In the Cisco IPCC Enterprise Web Administration window, browse to **IPCC Enterprise > Agent Management > Agents**.
4. In the Agents section, click the agent name to view the details. Alternately, create a new agent by clicking Create.

**Configuring skill groups**

A skill group is created in Unified CCE for mapping to user groups in Cisco Interaction Manager. You can create two types of skill groups:

- **Cisco Interaction Manager picks the agent (Non-IPTA):** For a Non-IPTA skill group, the skill group members (agents) are administered and managed in Cisco Interaction Manager. A Non-IPTA skill group is created for email routing in cases where a label is returned by Unified CCE to Cisco Interaction Manager. When a label is returned, Cisco Interaction Manager load balances the email activity to a group of agents defined in the user group (that maps to the Non-IPTA skill group) identified by the suffix of the label.
ICM-picks-the-agent (IPTA): For an IPTA skill group, the skill group members (agents) are administered and managed in Unified CCE. An IPTA skill group (with associated skill group members) is used in ICM scripts to facilitate email routing through Unified CCE to the skill group.

To configure a skill group:

1. Type the URL https://[Unified_SCCE_Server_Name]/uiroot/default/ipccAdmin/loginAdmin.jsp in your browser.
2. In the Login window, type the Administrator desktop login name and password. Click the Login button.
3. In the Cisco IPCC Enterprise Web Administration window, browse to IPCC Enterprise > Agent Management > Skill Groups.

Browse to Skill Groups node

4. In the Skill Groups section, click the skill group name to view the details. Alternately, create a new skill group by clicking Create.

View skill group details
Configuring call types

To configure a call type:

1. Type the URL https://unified_SCCE_Server_Name/uiroot/default/ipccAdmin/loginAdmin.jsp in your browser.

2. In the Login window, type the Administrator desktop login name and password. Click the Login button.

3. In the Cisco IPCC Enterprise Web Administration window, browse to IPCC Enterprise > Contact Management > Call Types.

4. In the Call Type section that appears, click the call type name to view the details. Alternately, create a new call type by clicking Create.
Configuring dialed numbers

To configure a dialed number:

1. Type the URL `https://Unified_SCCE_Server_Name/uiroot/default/ipccAdmin/loginAdmin.jsp` in your browser.

2. In the Login window, type the Administrator desktop login name and password. Click the **Login** button.

3. In the Cisco IPCC Enterprise Web Administration window, browse to **IPCC Enterprise > Contact Management > Dialed numbers**.

   ![Image of Cisco IPCC Enterprise Web Administration]

   **Browse to Dialed Numbers node**

4. In the Dialed numbers section, click the dialed number name to view the details. Alternately, create a new dialed number by clicking **Create**.

   ![Image of Cisco IPCC Enterprise Web Administration]

   **View dialed number details**
Configuring Network Interactive Voice Responses

To configure a network interactive voice response:

1. Type the URL `https://Unified_SCCE_Server_Name/uiroot/default/ipccAdmin/loginAdmin.jsp` in your browser.

2. In the Login window, type the Administrator desktop login name and password. Click the Login button.

3. In the Cisco IPCC Enterprise Web Administration window, browse to IPCC Enterprise > IVR Management > Network IVR.

4. In the Network IVR section, view the preconfigured Network IVRs. If required, edit them and click Save.

View Network IVR details

Configuring media routing domains

To configure a media routing domain:

1. Type the URL `https://Unified_SCCE_Server_Name/uiroot/default/ipccAdmin/loginAdmin.jsp` in your browser.

2. In the Login window, type the Administrator desktop login name and password. Click the Login button.

3. In the Cisco IPCC Enterprise Web Administration window, browse to IPCC Enterprise > Multichannel Management > Media routing domains.
4. In the Media routing domains section, click the MRD name to view the details. Alternately, create a new MRD by clicking Create.

Configuring scripts

For details on configuring a script see, “Configuring scripts” on page 29.
Installing Cisco Interaction Manager and the integration

To install Cisco Interaction Manager and the integration with Unified CCE:

1. Ensure that Microsoft SQL Server 2000 Service Pack 4 is installed and running on the machine on which you will be installing the Cisco Interaction Manager database.

2. From the Cisco Interaction Manager Environment CD, copy the BEA folder to a local directory on the Cisco Interaction Manager application server, and the JRE_1.6 folder to the user desktop.

3. From the BEA folder inside the local directory, open the folder WebLogic Server 8.1 SP6, and double-click the .exe file within it. This launches the installation process for WebLogic 8.1 SP 6 on the application server. Refer to WebLogicServerInstallGuide.pdf inside the BEA\documentation folder for steps to install and configure BEA WebLogic 8.1 SP 6.

4. From the JRE_1.6 folder inside the user desktop, double-click the .exe file. This launches the installation process for Sun JRE 1.6. Refer to readme.txt for instructions to install Sun JRE 1.6.

5. Install Cisco Interaction Manager. Refer to Cisco Unified Web and E-Mail Interaction Manager Installation Guide for Unified CCE for a detailed list of deployment options and installation steps corresponding to each deployment.

   The document also guides you through the procedure of setting up the integration. See the section “Integrating Unified WIM and Unified EIM with Unified CCE.”

6. From the Windows Services panel, start the Cisco Interaction Manager Service, and wait for 2–3 minutes before launching the URL to allow all the application services to start.

7. Configure the browser on user desktops according to the procedures detailed in the Cisco Unified Web and E-Mail Interaction Manager Browser Settings Guide.

Configuring objects in Cisco Interaction Manager

This section describes the following procedures:

1. “Verifying mapping of objects in the Administration Console” on page 47.

2. “Setting up knowledge base articles for Unified EIM” on page 50.

3. “Setting up business objects in the Administration Console” on page 52.

4. “Setting up services in the System Console” on page 55.

5. “Setting up web links for chat” on page 62.
Verifying mapping of objects in the Administration Console

To verify that Unified CCE objects have been mapped correctly in the Cisco Interaction Manager Administration Console:


2. Log in as the partition administrator (user name and password that were configured during the installation of Cisco Interaction Manager).

3. Select the Administration Console.
4. Under Partition, browse to **Settings**. Locate the **Application Instance** communication setting. Verify that it is set to the value chosen at the time of running the Unified CCE integration wizard.

Verify that **Application Instance** setting is correctly configured

5. Now locate the **MR Connection Port** communication setting. Enter the connection port for the External Agent Assignment service (EAAS) to listen to connections from the MR PIM via the MR interface. The value needs to match the value entered at the time of configuring MR PIM, which is configured during the Unified CCE installation. This is an important setting to ensure that activities are routed correctly through Unified CCE.

Configure **MR Connection Port** setting
6. Under the appropriate department, click the **User > Users** node in the Administration tree, to verify that all agents and supervisors which were selected at the time of running the integration wizard, are displayed.

**Review mapped users**

7. Under the appropriate department, click the **User > Groups** node in the Administration tree to verify that all skill groups, which were selected at the time of running the integration wizard, are displayed.

**Review mapped user groups**
8. Under the appropriate department, click the **Workflow > Queues** node in the Administration tree, and verify that all MRDs which were selected at the time of running the integration wizard, are displayed.

```
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Active</th>
<th>Default chat transfer queue</th>
<th>EPC/SCM Media Routing On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exception_Ques_Servic e</td>
<td>Exception_Ques</td>
<td>Yes</td>
<td>No</td>
<td>NA</td>
</tr>
<tr>
<td>EIM_Q</td>
<td>External Assignment Queue</td>
<td>Yes</td>
<td>No</td>
<td>Email_MRD_1</td>
</tr>
<tr>
<td>CPQ_Q</td>
<td>Internal Queue</td>
<td>Yes</td>
<td>No</td>
<td>NA</td>
</tr>
<tr>
<td>Default_Chat_Transfer_Ques...</td>
<td>Default_Chat_Transfer_Ques...</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
</tr>
</tbody>
</table>
```

**Review mapped queues**

### Setting up knowledge base articles for Unified EIM

The knowledge base (KB) consists of articles organized into folders. It includes certain standard folders to hold articles meant for specific use in emails, such as headers, greetings, signatures, and footers. Folders for articles of other types are created by KB managers and authors.

See [*Cisco Unified Web and E-Mail Interaction Manager Knowledge Base Console User’s Guide*](#) for the details of the procedures mentioned in this section.

**To set up KB articles for Unified EIM:**

2. Log in as the partition administrator.
3. Open the Knowledge Base Console.
4. In the Knowledge Base tree, browse to **Department > Shared > Standard > Email**. Create an article in each of the sub-nodes to set up one option each for a header, greeting, signature, and footer that can be used in responses to incoming activities in the department. Set up macros for the articles to make it easy to insert them into other articles or email responses.

Create a header, greeting, signature, and footer

5. Browse to the **Department > Shared** folder. Create a folder for auto-acknowledgements.

Create a folder for auto-acknowledgements
6. In the newly created folder, create an article for use in auto-acknowledgement emails. Use macros to insert the header, greeting, signature, and footer created earlier. These macros expand to the actual content at runtime.

Create a KB article to use in auto-acknowledgement emails

This article will be used later in a workflow (see page 53).

Setting up business objects in the Administration Console

See Cisco Unified Web and E-Mail Interaction Manager Administration Console User’s Guide for the details of the procedures mentioned in this section.

Unified EIM objects

To set up Unified EIM business objects in the Administration Console:

2. Log in as the partition administrator.
3. Open the Administration Console.
4. In the Administration tree, browse to the Email > Aliases node. Create an alias to serve as the entry point for emails into the system.

Create an email alias

5. Next, browse to the Workflow > Queues node to create an email queue.

Important: Skip this step if you intend to use only queues mapped to MRDs.

6. Then browse to the Workflow > Workflows > Inbound node to create an inbound workflow for this alias. The workflow will route incoming emails. Add the alias created in step 4 to the Start node. Add a queue mapped to MRD or the queue created in step 5 to the Queue node. Select the auto-acknowledgement KB article created earlier (see page 52) for the auto-acknowledgement node.

Create an inbound workflow
Unified WIM objects

To set up Unified WIM business objects in the Administration Console:

2. Log in as the partition administrator.
3. Open the Administration Console.
4. Next, browse to the Workflow > Queues node to create a chat queue.

   Important: Skip this step if intend to use only queues auto-configured from CSQs.

5. Browse to the Chat > Templates node. Create a new template set, and provide default messages for different states associated with a chat session, e.g., abandon, exit, error, and so on.

   Create a customer template set for chat
6. Browse to the **Chat > Entry Points** node. Create a new chat entry point by assigning the appropriate customer chat template. To route chats that enter from this entry point, use an auto-configured CSQ or the queue created in step 4. Make the entry point active.

---

**Set up an entry point for chats**

In the Properties pane, click the **Show HTML** button. The code used to generate a chat hyperlink to that entry point is displayed. Copy this link code into a Notepad file. Edit the code as explained in the Administration Console Help.

---

**Setting up services in the System Console**

Service processes are managed at the system level as shared resources across partitions. Service instances are managed within partitions.

See *Cisco Unified Web and E-Mail Interaction Manager System Console User's Guide* for the details of the procedures mentioned in this section.

---

**Unified EIM services**

This section helps you set up processes and instances for the following services:

- **Retriever**: Gets incoming emails from configured aliases and parses them.
- **Workflow Engine**: Applies workflows on emails to automate their routing and handling.
- **Dispatcher**: Sends outgoing emails out of the system.
To set up Unified EIM services in the System Console:

1. Open a new browser window, and launch the URL: http://Cisco_Interaction_Manager_Server/system. Log in as the system administrator (user name and password that were configured during the installation of Cisco Interaction Manager).

2. Select the System Console.

3. Browse to the Partitions > Partition > Services > Retriever node. Click the Retriever instance to use in the partition, and select the email alias that you had created earlier in the Administration Console (see page 53).

Associate a Retriever instance with the email alias created earlier
4. Restart the Retriever process and instance based on the notification message that appears. Browse to **Shared Resource > Services > Retriever**, and stop and start the Retriever process for the system.

5. Navigate back to the **Partitions > Partition > Services > Retriever** node. Stop and start the Retriever instance.
6. Browse to **Shared Resource > Services > Workflow > Workflow Engine** and verify that the Workflow Engine process is running. If the process is in a stopped state, start the process by clicking the **Run** button.

```
Verify that the Workflow Engine process is running
```

7. Browse to **Partitions > Partition > Services > Workflow > Workflow Engine** and start the Workflow Engine instance.

```
Start the Workflow Engine instance
```
8. Browse to **Shared Resource > Services > Email > Dispatcher** and verify that the Dispatcher process is running. If the process is in a stopped state, start the process by clicking the **Run** button.

Verify that the Dispatcher process is running

9. Browse to **Partitions > Partition > Services > Email > Dispatcher** and start the Dispatcher instance.

Start the Dispatcher instance
10. Browse to **Shared Resource > Services > Listener > Listener** and verify that the Listener process is running. If the process is in a stopped state, start the process by clicking the **Run** button.

**Verify that the Listener process is running**

11. Browse to **Partitions > Partition > Services > Listener > Listener**. Configure the Listener instance by providing the primary CTI server IP address and port number, and the secondary CTI server IP address and port number (optional) in the format, **CTI Server IP address: port number**. The start the Listener instance.

**Configure and start the Listener instance**
12. Browse to **Shared Resource > Services > EAAS > EAAS** and verify that the EAAS process is running. If the process is in a stopped state, start the process by clicking the Run button.

![Image of System Console with EAAS process and properties]

**Verify that the EAAS process is running**

13. Browse to **Partitions > Partition > Services > EAAS > EAAS** and start the EAAS instance.

![Image of System Console with EAAS instance properties]

**Start the EAAS instance**

Unified EIM is now ready for use. To verify, log in as an agent, supervisor, or administrator and perform basic tasks.

**Unified WIM services**

This section helps you set up processes and instances for the following service:

- **Agent Assignment**: Routes chats to agents.

**To set up Unified WIM services in the System Console:**

1. Open a new browser window, and launch the URL: `http://Cisco_Interaction_Manager_Server/system`.
2. Log in as the system administrator.

3. Browse to **Shared Resource > Services > Chat > Agent Assignment** and verify that the Agent Assignment process is running. If the process is in a stopped state, start the process by clicking the **Run** button.

4. Browse to **Partitions > Partition > Services > Chat > Agent Assignment** and start the Agent Assignment service instance.

**Setting up web links for chat**

**To create a chat link on your web site:**

- Open the code view of the host web page and add the edited link code (see page 55) from the entry point properties at the appropriate point. You may need to ask your web master to perform this task.

Unified WIM is now ready for use. To verify, log in as an agent or supervisor, and perform basic tasks.
Related documentation

Refer to the following Cisco Interaction Manager User’s Guides (for the Unified CCE integration) for more information about configuring and using Cisco Interaction Manager.

- Cisco Unified Web and E-Mail Interaction Manager Administration Console User’s Guide helps administrators set up and manage business objects.
- See Cisco Unified Web and E-Mail Interaction Manager System Console User’s Guide helps system administrators set up and manage services, loggers, and system monitors.
- See Cisco Unified Web and E-Mail Interaction Manager Tools Console User’s Guide helps business analysts extend the system by adding custom attributes. The Tools Console also enables administrators to configure screens and views for users and groups.
- See Cisco Unified Web and E-Mail Interaction Manager Reports Console User’s Guide helps managers and supervisors to set up and run reports to analyze various aspects of the system.
- See Cisco Unified Web and E-Mail Interaction Manager Knowledge Base Console User’s Guide helps knowledge base (KB) managers and authors to create and publish KB articles.
This chapter will assist you in understanding how to configure and maintain your Unified WIM and Unified EIM web servers.

- Configuring pool thread limit
This chapter will assist you in understanding how to configure and maintain your Unified WIM and Unified EIM web servers.

**Configuring Internet Information Services**

This procedure helps eliminate 503 errors on the web server.

**To configure Internet Information Services (IIS) on the web server:**

1. On the web server, go to **Start** menu > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

2. In the navigation tree, go to **Application Pools** > **DefaultAppPool**. Right-click the node and select **Properties**.

3. In the DefaultAppPool Properties window, on the Recycle tab, clear the following options:
   - Recycle worker process (in minutes)
4. On the Performance tab, clear the following options:
   - **Shutdown worker process after being idle for**
   - **Limit the kernel request queue**

5. On the Health tab, clear the following options:
   - **Enable pinging**
   - **Enable rapid fail protection**
Click **Apply**. Then click **OK** to close the window.

![Default AppPool Properties](image)

*Clear the Enable pinging and Enable rapid fail protection options*

## Configuring pool thread limit

This procedure increases the capacity of IIS to handle concurrent requests.

**To configure pool thread limit:**

1. On the machine where the web server associated with the primary application server is installed, go to **Start** menu > **Run**.
2. Type: `Regedit`  
   Press the Enter key.
3. In the Registry Editor window, navigate to `HKEY_LOCAL_MACHINE > System > CurrentControlSet > Services > InetInfo > Parameters`.

![Registry Editor](image)

*Navigate to InetInfo parameters*
4. Go to Edit menu > New > DWORD Value.
5. Change the name of the new registry value that gets created to PoolThreadLimit.
6. Right-click PoolThreadLimit and select Modify.
7. In the Edit DWORD Value window, set properties as following:
   - **Value data**: ffffffff
   - **Base**: Hexadecimal

   *Important: Make sure you have typed “f” eight times.*

8. Restart the server.
Managing application servers

- This chapter will assist you in understanding how to configure and maintain your Unified WIM and Unified EIM application servers.
- Routine maintenance tasks
This chapter will assist you in understanding how to configure and maintain your Unified WIM and Unified EIM application servers.

**Configuring WebLogic**

This procedure increases the application’s capacity to handle concurrent requests from users.

**Primary application server**

To configure the size of HTTP request queues for the primary application server:

1. Open `Cisco_Home\config\weblogic\config_Primary_Application_Server.xml`.
2. Locate the following line:
   ```xml
   <ExecuteQueue Name="default" ThreadCount="50" ThreadsIncrease="1"/>
   ```
   To ensure that an adequate number of threads have been allocated to the `default` pool, set the number of worker threads for WebLogic to at least 60% of the number of concurrent users. For example, if you have 100 concurrent users, set `ThreadCount` to 60; and if you have 150 users, set `ThreadCount` to 90.
3. Locate the following line:
   ```xml
   <ExecuteQueue Name="eGainPushletQueue" ThreadCount="50" ThreadsIncrease="1"/>
   ```
   Allocate an adequate number of threads to the pushlet queue. It should be 120% of the number of concurrent users.
4. Locate the following line:
   ```xml
   <Server XMLRegistry="MyXML Registry"
   ```
   In this line, after `Server`, add the following phrase:
   ```xml
   AcceptBacklog="100"
   ```
   The line should look like:
   ```xml
   <Server AcceptBacklog="100" XMLRegistry="MyXML Registry"
   ```
5. Locate the following line:
   ```xml
   <WebServer
   ```
   In this line, after `WebServer`, add the following phrase:
   ```xml
   KeepAliveSecs="120"
   ```
   That line should look like:
   ```xml
   <WebServer KeepAliveSecs="120"
   ```
6. Locate the following line:
   ```xml
   <ExecuteQueue Name="eGainLive" ThreadCount="50" ThreadsIncrease="1"/>
   ```
   Allocate an adequate number of threads to chat queues. It should be 120% of the number of concurrent chat sessions.

---

**Important:** Skip this step if your installation does not include Unified WIM.
Secondary application servers

To configure the size of HTTP request queues and connection parameters for secondary application servers:

1. Open \Cisco_Home\config\weblogic\config_Security_Application_Server.xml
2. Locate the following line:
   `<ExecuteQueue Name="default" ThreadCount="50" ThreadsIncrease="1"/>
   To ensure that an adequate number of threads have been allocated to the default pool, set the number of worker threads for WebLogic to at least 60% of the number of concurrent users. For example, if you have 100 concurrent users, set ThreadCount to 60; and if you have 150 users, set ThreadCount to 90.
3. Locate the following line:
   `<Server XMLRegistry="MyXML Registry"
   In this line, after Server, add the following phrase:
   AcceptBacklog="100"
   The line should look like:
   `<Server AcceptBacklog="100" XMLRegistry="MyXML Registry"
4. Locate the following line:
   `<WebServer
   In this line, after WebServer, add the following phrase:
   KeepAliveSecs="120"
   That line should look like:
   `<WebServer KeepAliveSecs="120"
5. Locate the following line:
   `<ExecuteQueue Name="eGainLive" ThreadCount="50" ThreadsIncrease="1"/>
   Allocate an adequate number of threads to chat queues. It should be 120% of the number of concurrent chat sessions.

Important: Skip this step if your installation does not include Unified WIM.

Routine maintenance tasks

Creating backup copies

- Back up the Cisco_Home folder regularly. Exclude the Log folder under Cisco_Home from the backup.
Archiving

- Purge archived activities to free up the disk space occupied by attachments of archived activities.
- Schedule archive jobs to run during your off-peak hours to avoid database performance bottlenecks.

Applying Microsoft security patches and service packs

Microsoft releases security patches and service packs to plug vulnerabilities in the operating system and various programs.

- Apply these patches after confirming their impact on the application.
Managing databases

- This chapter will assist you in understanding how to configure and maintain your Unified WIM and Unified EIM databases.
- Routine maintenance tasks
This chapter will assist you in understanding how to configure and maintain your Unified WIM and Unified EIM databases.

## Best practices for configuring databases

### Installation and settings

#### Active database
- While installing the application, ensure that data and log files of the active database reside on a disk volume with a good amount of free disk space.
- Set the active database properties as follows:
  - Properties of Datafile: Automatically grow file by 400-700 MB
  - Maximum file size set to unrestricted file growth

#### Other databases
- Other system databases (master, model, msdb, TEMPDB) should also be installed on a disk volume with a good amount of free disk space because TEMPDB may sometimes grow due to application requirements. Care needs to be taken during MSSQL installation that the data files are pointed to other location rather than the system volume.

#### Transaction logs
- Set the transaction log properties as follows:
  - Properties of Datafile: Automatically grow file by 10%
  - Maximum file size set to unrestricted file growth

### Optimal configuration settings

<table>
<thead>
<tr>
<th>Database configuration setting</th>
<th>Recommended value</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto_close</td>
<td>off</td>
</tr>
<tr>
<td>auto_create_statistics</td>
<td>on</td>
</tr>
<tr>
<td>auto_update_statistics</td>
<td>on</td>
</tr>
<tr>
<td>auto_shrink</td>
<td>off</td>
</tr>
<tr>
<td>read_only</td>
<td>off</td>
</tr>
</tbody>
</table>
Configuring anti-virus protection

Anti-virus protection is necessary, but enabling all files for virus scan may cause performance issues.

- Exclude .mdf, .ldf, .ndf, and .dat files from virus scan.

Routine maintenance tasks

Rebuilding indexes

Rebuilding of indexes enhances database performance.

- Run rebuild index jobs on a weekly basis during off peak hours.

Optimizing database file space

At times, the transaction log may grow considerably, especially if the recovery model of the database is set to "Full." Although the active portion of transaction logs is committed after checkpoint or truncated after transaction log backups, the free space within the transaction log file may not be released to the operating system. This could lead to disk space crunch.

- Run a space optimization job every day during off peak hours to release the free space within the transaction logs back to the operating system.

Performing disk defragmentation

- Weekly defragmentation is recommended. Note that it requires downtime.

Creating backup copies

Backups are critical in case of hardware failure. The following backup policy ensures that you won’t lose more than one hour of data. SQL supports full recovery model and hence this policy is strongly recommended. When
the recovery mode is set to full it is necessary to backup transactional logs periodically. Otherwise it may lead to a disk space issue because of transaction logs growing indefinitely.

- Perform a weekly complete backup, daily differential backup, and hourly transactional log backups.

Archiving

Regular archiving helps to keep the size of the database manageable. The maximum size of the database should be kept under 20 GB in most cases.

- Schedule archive jobs to run during your off-peak hours to avoid database performance bottlenecks.
- Purge archived activities to create more available disk space.

Applying Microsoft security patches and service packs

Microsoft releases security patches and service packs to plug vulnerabilities in the operating system and various programs.

- Apply these patches after confirming their impact on the application.
Managing Windows servers

- Best practices for configuring Windows servers
- Routine maintenance tasks
- Performance tuning considerations
This chapter will assist you in understanding how to configure and maintain your Unified WIM and Unified EIM servers.

**Best practices for configuring Windows servers**

**Allocating adequate virtual memory**

- Virtual memory setting should be set to 1.5 times the physical memory. It is also recommended to distribute the virtual memory across disk volumes to avoid space crunch on system volume during run time.

**Setting up disk space**

- All the system volumes should have more than 10% of their actual space free for application and other operating system (OS) related activities at any given time.

**Configuring anti-virus protection**

- As email attachments are prone to virus attacks, set up scanning of email attachments on your mail exchange server.

**Routine maintenance tasks**

**Monitoring disk space**

- Monitor and free space on disk volumes from time to time by deleting the unnecessary files. Installation programs, application logs, user profiles, Dr. Watson logs, temp files are known to occupy the space unnecessarily. However, if it is not possible to free disk space further because of the size of the data, the administrator should plan archiving of old data or migration of the system to a larger capacity server.

**Applying Microsoft security patches and service packs**

Microsoft releases security patches and service packs to plug vulnerabilities in the operating system and various programs.

- Apply these patches after confirming their impact on the application.
Performance tuning considerations

One of the first steps towards tuning an application is to determine evolving requirements, which is not easy as requirements are likely to vary across different types of users. Administrators, typically, want the system to be easily configurable for various user loads, security needs, and application uptime. Business managers tend to care about issues such as security considerations for critical data that is passed between various components within the application, response times, reliability, availability and scalability. For agents, response time is the most important factor that defines a finely tuned system.

Cisco Unified Web and E-Mail Interaction Manager Solutions Reference Network Design Guide helps you plan your configuration when you first set it up. In this section, we provide a quick overview of some of the factors that you should consider as the system grows.

Peak concurrent usage

The application will need to be tuned if there is a need to meet specific concurrent usage requirements. Concurrent usage includes usage by email and chat agents as well as chat sessions. The general guideline is that the greater the number of concurrent users, the likelier it is for the system to be stressed resulting in longer response times.

Email volume

The email volume that the application handles determines the amount of disk space used by the database, size of active and master databases, and the capacity of the database engine to provide optimal response times to data requests. Active usage of email attachments and Knowledge Base (KB) articles also affect disk space requirements.

Server configuration

It is a well known fact that the specifications for servers that run critical business application are constantly changing and, therefore, the application needs to account for such periodic changes. The server configuration and environment must be tailored to allow application to take advantage of it and vice versa. Therefore, if the server configuration is either downsized (less likely to occur) or increased (more likely), then the application needs to be tuned to the current server configuration. In addition, other applications that might be running on the same hardware also affect the tuning of the application.

Security requirements

Often security requirements dictate that the application data should be accessed in a secure way. For this reason secure sockets layer (SSL) mode of access to information is set up. Likewise, sharing and access to critical information such as customer data require that data is stored and retrieved in a secure way by extra access control and beyond.

Additional security requirements do lead to some delay in response times for users accessing the application. This should be clearly understood by administrators setting up SSL mode of access on web servers or trying to access information stored on remote and highly secure resources like remotely mounted file systems or disks.
See Cisco Unified Web and E-Mail Interaction Manager Installation Guide for information about how to set up the SSL mode of communication on the web server.