## Contents

### Preface
- About This Guide ................................................................. 8
- Document Conventions .......................................................... 8
- Other Learning Resources ...................................................... 9
  - Online Help ........................................................................ 9
  - Documentation ................................................................... 9

### Chapter 1: Preparing Unified CCE for the Integration
- Relationship Between Objects in Unified CCE and Unified EIM and WIM ........................................ 12
- Designing Your Installation ..................................................... 12
- Obtaining Unified EIM and WIM Licenses .................................. 12
- Installing Unified CCE ............................................................. 13
- Setting up Agent Desktops for Voice Call Routing ....................... 13
- Configuring Cisco Unified Communication Manager for Routing Voice Calls .......................... 14
- Planning Unified CCE Configuration ........................................ 18
- Configuring Unified CCE ........................................................ 19
  - Configuring Application Instance ......................................... 19
  - About Media Classes .......................................................... 20
    - Important Note About Media Classes ................................. 21
  - Configuring Media Classes .................................................. 21
  - Configuring Media Routing Domains (MRDs) ......................... 22
  - Configuring Network VRU ................................................... 24
  - Configuring Network VRU Scripts ........................................ 24
  - Configuring Call Types ........................................................ 25
  - Configuring Media Routing Peripheral Gateways (MR PGs) ....... 26
  - Configuring Agent Desk Settings ......................................... 30
  - Configuring Agent Peripheral Gateway (Agent PG) ................. 31
  - Configuring Network Trunk Group ....................................... 33
  - Configuring Application Path ............................................... 34
  - Configuring Agents ............................................................. 36
  - Configuring Skill Groups ..................................................... 37
## Chapter 2: Setting Up Integrated Objects

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Variables in Unified EIM and WIM</td>
<td>57</td>
</tr>
<tr>
<td>Verifying Mapping of Objects in the Administration Console</td>
<td>57</td>
</tr>
<tr>
<td>Setting Up Knowledge Base Articles for Unified EIM</td>
<td>58</td>
</tr>
<tr>
<td>Setting up Business Objects in the Administration Console</td>
<td>59</td>
</tr>
<tr>
<td>Unified EIM Objects</td>
<td>59</td>
</tr>
<tr>
<td>Unified WIM Objects</td>
<td>59</td>
</tr>
<tr>
<td>Setting Up Services in the System Console</td>
<td>60</td>
</tr>
<tr>
<td>Unified EIM Services</td>
<td>60</td>
</tr>
<tr>
<td>Unified WIM Services</td>
<td>61</td>
</tr>
<tr>
<td>Setting Up Web Links for Chat and Collaboration</td>
<td>62</td>
</tr>
<tr>
<td>Configuring Dynamic Messages for Integrated Chats</td>
<td>62</td>
</tr>
<tr>
<td>Handling Email Assignment</td>
<td>65</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>65</td>
</tr>
</tbody>
</table>

## Chapter 3: Managing and Maintaining Servers

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypting SQL Server Database</td>
<td>68</td>
</tr>
<tr>
<td>Best Practices for Configuring Servers</td>
<td>69</td>
</tr>
<tr>
<td>For All Servers</td>
<td>69</td>
</tr>
<tr>
<td>Allocating Adequate Virtual Memory</td>
<td>69</td>
</tr>
</tbody>
</table>
Extract Connection Pool File {egpl_ds_connpool_map.xml} ..................................... 84
  From the EAR ..................................................................................... 84
  From the Services Server .................................................................. 85
Update Connection Pool File {egpl_ds_connpool_map.xml} ................................. 85
  Changes to the EAR .......................................................................... 85
  Changes on the Services Server ......................................................... 86
Extract a Template From the EAR ............................................................... 86
Remove a Template From the EAR ............................................................ 86
Add or Update a Template in the EAR ....................................................... 87
Add Custom JARS Required for Customization ........................................... 87
  Changes to the EAR .......................................................................... 87
  Changes on the Service Server .......................................................... 88
Add New Custom Classes Required for Customization ................................. 88
  Changes to the EAR .......................................................................... 88
  Changes on the Service Server .......................................................... 89
Add New Java Data Adapter Classes Required for Customization ............... 89
  Changes to the EAR .......................................................................... 89
  Changes on the Service Server .......................................................... 90
Add New Query and Schema Files Required for Customization .................. 90
  Changes to the EAR .......................................................................... 90
  Changes on the Service Server .......................................................... 90
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 centers and customer service 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 Deployment and Maintenance Guide* discusses best practices for maintaining the Unified EIM and WIM installation. Intended for system and database administrators, this guide will help administrators to keep the installation in good health and to fine tune it to improve its performance.

This version of the guide is for installations that are integrated with Cisco Unified Contact Center Enterprise (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>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><em>Variable</em></td>
<td>User-specific text; varies from one user or installation to another.</td>
</tr>
</tbody>
</table>

**Document conventions**
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><strong>Help</strong> button</td>
<td>Topics in <em>Cisco Unified Web and E-Mail Interaction Manager Help</em>; the Help button appears in the console toolbar on every screen.</td>
</tr>
<tr>
<td><strong>F1</strong> 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)

The document set contains the following guides:

- *Hardware and System Software Specification for Cisco Unified Web and E-Mail Interaction Manager*
- *Cisco Unified Web and E-Mail Interaction Manager Solutions Reference Network Design Guide*
- *Cisco Unified Web and E-Mail Interaction Manager Installation Guide*
- *Cisco Unified Web and E-Mail Interaction Manager Browser Settings Guide*

User Guides for agents and supervisors

- *Cisco Unified Web and E-Mail Interaction Manager Agent’s Guide*
- *Cisco Unified Web and E-Mail Interaction Manager Supervisor’s Guide*

User guides for Knowledge Base managers and authors

- *Cisco Unified Web and E-Mail Interaction Manager Author’s Guide*
User guides for administrators

- Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Administration Console
- Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Routing and Workflows
- Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Chat and Collaboration Resources
- Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Email Resources
- Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Data Adapter
- Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Offers Console
- Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Reports Console
- Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to System Console
- Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Tools Console
Preparing Unified CCE for the Integration

- Relationship Between Objects in Unified CCE and Unified EIM and WIM
- Designing Your Installation
- Obtaining Unified EIM and WIM Licenses
- Installing Unified CCE
- Setting up Agent Desktops for Voice Call Routing
- Configuring Cisco Unified Communication Manager for Routing Voice Calls
- Planning Unified CCE Configuration
- Configuring Unified CCE
- Installing Cisco Media Blender
- Installing Unified EIM and WIM and the Integration
- Configuring the System for Multiple Agent PGs
- Configuring Finesse
This chapter provides an overview of the process of setting up an integrated Unified EIM and WIM–Unified CCE system. It includes a note about the relationship between objects in the two systems.

**Relationship Between Objects in Unified CCE and Unified EIM and WIM**

This section provides a brief introduction to the relationship or “mapping” between objects that are used in both Unified CCE and Unified EIM and WIM.

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 Unified EIM and WIM to</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Supervisor Administrator</td>
<td>User</td>
<td>▶ An agent belongs to a peripheral.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▶ A peripheral belongs to an agent peripheral gateway (PG).</td>
</tr>
<tr>
<td>Skill group</td>
<td>User group</td>
<td>▶ A skill group belongs to a peripheral.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▶ A peripheral belongs to an agent PG.</td>
</tr>
<tr>
<td>Media routing domain (MRD)</td>
<td>Queue</td>
<td>▶ Multiple queues can belong to a single MRD.</td>
</tr>
<tr>
<td>Script selector</td>
<td>Queue</td>
<td>▶ A script selector can belong to only one queue.</td>
</tr>
</tbody>
</table>

Typically, the mapping between these objects is initially set up by running the Cisco Interaction Manager integration wizard. The integration wizard can be run once for each department. Subsequently, additional objects can be created in Unified CCE and manually mapped to Unified EIM and WIM objects. This is done from the Unified EIM and WIM Administration Console.

Properties of mapped objects are set up in Unified CCE, while permissions are managed through Unified EIM and WIM.

**Designing Your Installation**

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

**Obtaining Unified EIM and WIM Licenses**

- To order licenses for the Unified EIM and WIM deployment, contact the Cisco License team. You will need licenses while setting up the integrated system.
Installing Unified CCE

- Ensure that Unified CCE is installed and available for use. Verify that the following items are installed:
  - Unified CCE Instance
  - Call Router Side A
  - Call Router Side B (optional)
  - Logger Side A
  - Logger Side B (optional)
  - Primary Admin Workstation
  - Secondary Admin Workstation (optional)
  - Historic Data Server
  - Network Interface Controllers (NIC) (Only required for Pre-routing)
  - Agent Peripheral Gateway (Agent PG)
  - Media Routing Peripheral Gateway (MR PG)
  - CTI Server
  - CUIC Database
  - Java Telephony Application Programming Interface (JTAPI)
  - Cisco Media Blender (CMB) (Only required for callback and delayed callback activities.)
  - Computer Telephony Integration Object Server (CTIOS) (Only required for callback and delayed callback activities.)
  - Cisco Finesse

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*

Setting up Agent Desktops for Voice Call Routing

- Install IP Communicator on each agent’s desktop, or configure an IP phone that communicates with Cisco Unified Communication Manager for the agent. Look at the following links for detailed instructions on installing and configuring IP Communicator and IP phones.
Configuring Cisco Unified Communication Manager for Routing Voice Calls

This section talks about how to configure phones, directory numbers, and end users from the Cisco Unified Communication Manager Administration user interface.

To configure Cisco Unified Communication Manager for routing voice calls:

1. Open a web browser and launch the URL: http://Cisco Unified Communication Manager Server Name.
2. On the page, click the link Cisco Unified Communications Manager Administration.
3. On the login page, provide the administrator username and password and click the Login button.

4. On the next page, from the Device menu, select Phone.
5. On the Find and List Phones page, click the Add New button.
6. On the Add a New Phone page, in the **Phone Type** field, select **Cisco IP Communicator** or the IP phone configured earlier on page 13. Click **Next**.

7. On the Phone Configuration page, in the **Select the device protocol** field, select **SCCP**. Click **Next**.
8. On the Phone Configuration page, provide the details for the new phone. Refer to Help > This Page for details about the fields. After providing all the required information, click the Save button.

9. Next, from the Call Routing menu, select Directory Number.

10. On the Find and List Directory Numbers page, click the Add New button.
11. On the Directory Number Configuration page, provide the details for the new directory number. Refer to Help > This Page for details about the fields. After providing all the required information, click the Save button.

Configure the directory number properties

12. Next, from the User Management menu, select End User.

13. On the Find and List Users page, click the Add New button.

Click the Add New button

14. On the End User Configuration page, provide the details for the new user. Refer to Help > This Page for details about the fields. After providing all the required information, click the Save button. Make sure you provide the following values in the Controlled Devices and Primary Extension fields.

- Controlled Devices: Select the phone configured in Step 8.
Primary Extension: Select the directory number configured in Step 11.

Ensure that the new agent phone is associated with the user that was created while installing the Agent PG. For details, see the Cisco Unified Contact Center Enterprise Installation Guide.

Planning Unified CCE Configuration

To integrate Unified CCE with Unified EIM and WIM, multiple objects have to be configured in Unified CCE. The specific objects that have to configured will depend on the activities (email, chat etc.) supported by the integrated installation. This section describes the objects required for each activity type—inbound email, outbound email, chat, callback, and delayed callback.

The following objects must be configured in the order in which they are presented here. For configuration details, refer to the following section: “Configuring Unified CCE” on page 19.

1. Application instance (page 19)
2. Media classes (page 21)
3. Media routing domains (MRD) (page 22)
4. Network voice response unit (Network VRU) (Not required for outbound email activities) (page 24)
5. Network voice response unit script (Network VRU script) (Not required for inbound email and outbound email activities) (page 24)
6. Call type (page 25)
7. Media routing peripheral gateway (MR PG) (page 26)
8. Agent desk settings (page 30)
9. Agent peripheral gateway (Agent PG) (page 31)
10. Network trunk group (page 33)
11. Application path (page 34)
12. Agents (page 36)
13. Skill Groups
   - IPTA skill groups (page 38)
   - Non-IPTA skill group (Not required for callback and delayed callback activities.) (page 39)
14. Labels (Not required for callback and delayed callback activities.) (page 41)
15. Script selector (page 42)
16. Scripts (Not required for outbound email activities) (page 44)
17. Device target (Not required for inbound email, outbound email, and chat activities) (page 49)
18. Expanded Call Context (ECC) variables (page 50)
19. Cisco Finesse (page 53)

Configuring Unified CCE

This section describes the process of configuring Unified CCE objects that are required for the integration with Unified EIM and WIM. These objects must be configured in the order in which they are presented here. For details of these objects refer to the Online Help and printed documentation for Unified CCE.

Configuring Application Instance

Application instances are configured for each installation of a multi-media feature in the configuration.

Configure a single application instance for integrating with Unified EIM and WIM. This application instance is used for inbound email, outbound email, chat, callback, and delayed callback activities.

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. Please note that Unified EIM and WIM uses the application instance name and not the application key to connect to Unified CCE.
- **Application type**: Set it to `<Other>`.
- **Permission level**: Set it to **Read only**.

Click **Save**.

![Configure the application instance](image)

### About Media Classes

A media class defines the type of requests you want to set up for routing on Unified CCE. Configure a media class for each media supported by the Unified EIM and WIM deployment. A media class is required for creating MRDs. It helps categorize the MRDs based on media type (email, for example).

Create the following media classes:

- An email media class for inbound emails.
- An email media class for outbound emails.
- A chat media class for chat.
- Callback and Delayed callback use the existing `cisco_voice` media class, which is already created by the system.

Once a media-class for a particular media is created, all other objects required for that media class must also be configured.
Important Note About Media Classes

If the deployment does not require one or more of these media classes and the administrator does not wish to create it or its associated objects, complete the following steps before starting the application:

1. On the Cisco Interaction Manager active database, run the following query to find out the current value of the media class properties.

   ```sql
   select * from egpl_config_property where domain='ipcc.egicm_media_class_mappings.properties'
   ```

   Run the query on the active database

2. Comment out the name of the media class, for example, CIM_BC, by adding the # sign in front of the media class name. For example, run the following query on the active database to change the CIM_BC property.

   ```sql
   Update egpl_config_property set Name='#CIM_BC' where domain='ipcc.egicm_media_class_mappings.properties' and NAME = 'CIM_BC'
   ```

Configuring Media Classes

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. If the media class is meant to be used in Unified EIM and WIM, use one of the following names. Note that the names of media classes are case sensitive. Make sure that you use the exact names as provided here.
- CIM_EIM (for inbound email)
- CIM_OUTBOUND (for outbound email)
- CIM_WIM (for chat)

Media classes are set in the active database table `egpl_config_property` table as CIM_EIM, CIM_OUTBOUND, and CIM_WIM. If you use names other than these, you must change them in the database and then restart the Cisco Service. Note that the names of media classes are case sensitive.

In the Task section, set the following.
- **Life**: Set the value to 300 seconds.
- **Start timeout**: Set the value to 30 seconds.
- **Max Duration**: Set the value to 28800 seconds.

6. Click **Save**.

![Configure media classes](image)

### Configuring Media Routing Domains (MRDs)

An MRD is a collection of skill groups and services that are associated with a common communication medium. Unified CCE uses an MRD to route tasks to agents who are associated with a skill group and a particular medium. A media routing domain is created in Unified CCE for mapping to queues in Unified EIM and WIM.

Create the following media routing domains:
- For inbound email media class, create an email media routing domain.
- For outbound email media class, create an email media routing domain.
- For chat, create a chat media routing domain.
- For callback and delayed callback, use the existing voice media routing domain (`Cisco_Voice`) created by the system.
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 (page 21). Make sure that you select the correct media class for the MRD. For example:
     - For inbound email MRD, select the CIM_EIM media class.
     - For outbound email MRD, the CIM_OUTBOUND media class.
     - For chat MRD, select the CIM_WIM media class.
   - **Interruptible**: Select this option while creating MRDs for inbound and outbound emails.

In the Calls in Queue section, set the following:

- **Max**: Defines the maximum number of activities to be queued for the MRD. The recommended value for this setting is 5000. However, the maximum value for email activities can be set to 15000. For all other activities, this value should not be set more than 5000. If the field is left blank, Unified EIM and WIM will read the value from the active database table egpl_config_property. By default the value of the DEFAULT_MAX_CALLS_IN_MRD property is set to 5000.

6. Click Save.
Configuring Network VRU

A Network VRU is required for supporting incoming activities to Unified CCE. Note that this Network VRU configuration has no relationship with any physical Network VRU existing in your environment.

Configure a single Network VRU for Unified EIM and WIM. This network VRU is used by inbound email, chat, callback, and delayed callback activities. It is not required for outbound email activities.

**To configure a Network 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.**
3. Double-click **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.**

![Configure network VRU](image)

6. Click **Save.**

Configuring Network VRU Scripts

Configure Network VRU scripts if you want to display dynamic content to chat customers (for example, wait time, activity ID, etc) while chat requests are being processed by the system. This is an optional feature. The
Preparing Unified CCE for the Integration

Dynamic messages are configured in Unified EIM and WIM (See page 62 for details). The name of the Network VRU script that is configured here is used while configuring the dynamic messages.

Network VRU scripts need to be configured only for chat, callback, and delayed callback activities.

**To configure a Network VRU script:**

1. Go to Start > All Programs > ICM Admin Workstation > Configuration Manager.
2. In the Configuration Manager window, browse to Tools > List Tools > Network VRU Script List.
3. In the Network VRU Script List window, create a script and select the Network VRU created for Unified WIM and EIM (page 24).
4. Click the Save button.

**Configuring Call Types**

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

Individual call types are required for the following activities: inbound email, outbound email, chat, callback, and delayed callback activities. Make sure you complete these steps for each type of activity.

**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**.

![Call Type List window](image)

**Provide the name of the call type**

### Configuring Media Routing Peripheral Gateways (MR PGs)

An MR PG handles new activity routing requests initiated by Unified EIM and WIM, over the connection established by the embedded MR PIM (side A or side B). The MR PG provides routing instructions to Unified EIM and WIM, while the Agent PG is used to report agent state and status to Unified CCE. Also note that agents are not configured on MR PG. They are always configured on the Agent PG.

Configure a single MR PG for Unified EIM and WIM. This MR PG is used for inbound email, outbound email, chat, callback, and delayed callback activities.

The MR PG configuration involves three steps:

- Configuring MR PG using the Configuration Manager: The details are described in this section.
- Installing MR PG: For details, see the Unified CCE Installation Guide.
- Creating MR PIM for the installed MR PG: You need to create a single MR PIM for Unified EIM and WIM. For details, see the Unified CCE Installation Guide. While creating the MR PIM, you are asked to provide the Application Connection Port number. As a best practice, use a port number that is greater than 2000. This port number is required while configuring the External Agent Assignment Server (EAAS) (page 61).

#### 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**.

![Configure an MR PG]

6. Click [2] **Add Peripheral**.
   A new set of tabs appear.

7. On the Peripheral tab, provide the following details:
   - **Client type**: Select **MR PG**.
   - **Default desk settings**: Select **None**.
Enable Post Routing: Select the option.

8. On the Advanced tab, in the **Network VRU** field, from the dropdown list, select the Network VRU configured for Unified EIM and WIM (page 24).

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 *None*.
- **Default call type:** From the dropdown list, select *None*.
- **Client type:** Set it to MR PG.

Click Save.

10. On the Default route tab, in the **Media Routing Domain** field, ensure that the Route: field is set to None.
11. Click Save. Note down the Logical controller ID generated in the Logical Controller tab. It is needed while configuring MR PIM.

Important: Now install the MR PG and configure the MR PIM. For more information, see the Unified CCE Installation Guide.

Configuring Agent Desk Settings

Agent desk settings are a common set of properties for a group of agents working on voice call requests. This is required for configuring an Agent PG. At least one Agent Desk Setting must be configured for Unified EIM and WIM.

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.

Provide the name of the agent desk settings group
Configuring Agent Peripheral Gateway (Agent PG)

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

You can configure a maximum of four Agent PGs for Unified EIM and WIM. These Agent PGs are used for inbound email, outbound email, chat, callback, and delayed callback activities.

Note that you can also use an existing Agent PG if it is of the type Call Manager/Soft ACD.

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 or PG Generic.
   - **Primary CTI address**: Provide the address of the primary CTI server in the format IP_Address:Port_Number. You can either provide the IP address, or the host name.
   - **Secondary CTI address**: Provide the address of the secondary CTI server in the format IP_Address:Port_Number. You can either provide the IP address, or the host name. The secondary CTI address is needed only if the Unified CCE system is duplexed.
   A new set of tabs appear.
7. On the Peripheral tab, do the following:
   - **Default desk settings**: From the dropdown list, select the agent desk settings configured for Unified EIM and WIM (page 30).
   - **Enable post routing**: Select the option.

8. On the Routing client tab, in the **Name** field, provide a name for the routing client.

9. 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.
10. Click Save.

Configure agent distribution

Configuring Network Trunk Group

Individual network trunk groups are required for the following activities: inbound email, outbound email, chat, callback, and delayed callback activities. Complete these steps for each type of activity.

To configure a network trunk group:

1. Go to Start > All Programs > ICM Admin Workstation > Configuration Manager.
2. In the Configuration Manager window, browse to Tools > Explorer Tools > Network Trunk Group Explorer.
3. In the Network Trunk Group window, in the Select filter data section, in the PG field select an agent peripheral. Click Retrieve.
4. Click the [1] Add Network trunk group button.
5. On the Network Trunk Group tab, in the Name field, provide the name of the network trunk group.
7. On the trunk Group tab, set the following.
   - **Peripheral**: From the dropdown list, select an agent peripheral configured for Unified EIM and WIM (page 31).
   - **Peripheral number**: Provide a unique peripheral number.
   - **Peripheral name**: Provide a unique peripheral name.
   - **Name**: This field is auto-populated.
9. On the Trunk tab, in the **Trunk type** field, select **DND/DNIS**.

10. Click **Save**.

---

**Configure a network trunk group**

### Configuring Application Path

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

Create a single application path and add all the MRD-peripheral combinations for the Agent PG to the application path member list. You do not need to add the voice MRD (Cisco_Voice) to this list. The application path is used for inbound email, outbound email, chat, callback, and delayed callback activities.

Access to the application object filter is restricted. Log in as a super user to enable or disable the application object filter. For details about the super user password, see the **Configuration Guide** for Cisco Unified ICM/Contact Center Enterprise and Hosted available at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guides_list.html

#### To configure an application path:

1. Go to **Start > All Programs > ICM Admin Workstation > Configuration Manager**.
2. In the Configuration Manager window, go to **Options > Application Object Filter**.
3. In the Application Object Filter window, in the Disable / Enable application object filter section, in the **Superuser password** field, provide the password of the superuser and click the **Disable** button. Click **OK**.

![Application Object Filter](image)

*Provide the password of the superuser*

4. In the Configuration Manager window, browse to **Tools > List Tools > Application Path List**.

5. Double-click **Application Path List**.

6. In the Application Path List window, in the Select filter data section, in the Application Instance field select the application instance configured for Unified EIM and WIM (page 19). Click **Retrieve**.

7. In the Application Path section, click **Add**.

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

8. On the Attributes tab, provide the following details:
   - **Application Instance**: From the dropdown list, select the application instance configured for Unified EIM and WIM (page 19).
   - **Peripheral Gateway**: From the dropdown list, select an agent peripheral gateway configured for Unified EIM and WIM (page 31).
   - **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 EIM and WIM (page 31).
   - **Media routing domain**: From the dropdown list, select an MRD configured for Unified EIM and WIM (page 22).

   Add all the MRD-peripheral combinations for the Agent PG to the application path member list. You do not need to add the voice MRD (**Cisco_Voice**) to this list.
**Configure application path**

9. In the Configuration Manager window, go to **Options > Application Object Filter.**

10. In the Application Object Filter window, in the Disable / Enable application object filter section, click the **Enable** button. Click **OK.**

---

**Configuring Agents**

An agent is created in Unified CCE for mapping to users in Unified EIM and WIM. Create all IPTA and Non-IPTA agents for whom routing or reporting is done in Unified CCE.

Create agents for handling inbound email, outbound email, chat, callback, and delayed callback activities.

**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, in the **Peripheral** field select an agent peripheral. Click **Retrieve.**

5. Click the **[1]Add Agent** button.

A new entry is created and a new set of tabs appear.

6. On the Agent tab, provide the following details:
   - **First name:** Provide the first name.
   - **Last name:** Provide the last name.
Preparing Unified CCE for the Integration

- **Login name:** Provide the login name for the agent. For callback and delayed callback agents, the login name should match the User ID provided while configuring End users from the Cisco Unified Communication Manager Administration user interface (page 17).
- **Login enabled:** Select the option.
- **Password:** Provide the password for the agent.
- **Enterprise name:** This field is auto-populated.

7. Click **Save**.

---

**Configuring Skill Groups**

A skill group is created in Unified CCE for mapping to user groups in Unified EIM and WIM. You can create two types of skill groups:

- **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 scripts to facilitate routing through Unified CCE to the skill group. This is used for inbound email, outbound email, chat, callback, and delayed callback activities.

- **Unified EIM and WIM picks the agent (Non-IPTA):** For a Non-IPTA skill group, the skill group members (agents) are administered and managed in Unified EIM and WIM. A Non-IPTA skill group is created for routing activities in cases where a label is returned by Unified CCE to Unified EIM and WIM. When a label is returned, Unified EIM and WIM load balances the 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. This can be used for inbound email, outbound email, and chat activities.

---

**Important:** Users can only belong to either IPTA or Non-IPTA skill groups. Ensure that the same user is not added to an IPTA and a Non-IPTA 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.
4. In the Skill Group Explorer window, in the Select filter data section, select an agent peripheral. Click Retrieve.
5. Click the [1]Add Skill group button.
   A new entry is created and a new set of tabs appear.
6. On the Skill Group tab, provide the following details:
   - **Media routing domain**: From the dropdown list, select an MRD configured for Unified EIM and WIM (page 22).
   - **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.

7. 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.

8. Click the Add Route button.

A new tab appears.

9. 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.
4. In the Skill Group Explorer window, in the Select filter data section, select an agent peripheral. Click Retrieve.
5. Click the [1]Add Skill group button.

A new entry is created and a new set of tabs appear.
6. On the Skill Group tab, provide the following details:
   - **Media Routing Domain**: From the dropdown list, select an MRD configured for Unified EIM and WIM (page 22).
   - **Peripheral Name**: Provide a name for the skill group.
   - **Name**: This field is auto-populated.
   - **ICM picks the agent**: Clear the option.

   Click **Save**.

7. Click the **Add Route** button.

   A new tab appears.

8. On the Route tab, do the following:
   - **Name**: Provide the name for the route.

   Click **Save**.

---

*Configure a Non-IPTA skill group*
Provide the name of the route

Configuring Labels

Labels are used by Unified EIM and WIM for Non-IPTA routing. When Unified CCE is unable to identify an agent for assigning an activity, it returns a label to Unified EIM and WIM. When a label is returned, Unified EIM and WIM load balances the 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.

Configure labels for inbound email, outbound email, and chat activities.

Important: The LABEL must be configured in the following format: LBL_Enterprise_Name_of.Non-IPTA_skill_Group. The names of labels are case sensitive.

To configure a label:

1. Go to Start > All Programs > ICM Admin Workstation > Configuration Manager.
2. In the Configuration Manager window, browse to Tools > List Tools > Label List.
3. Double-click Label List.
4. In the Label List window, in the Select filter data section, in the Routing client field select the routing client configured for MR PG (page 28). Click Retrieve.
5. In the Label 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 the routing client configured for the MR PG in step 9 in “Configuring Media Routing Peripheral Gateways (MR PGs)” on page 26.
Label: Provide a name for the label that can be used in a script for Non-IPTA routing. The label must be configured in the following format: LBL_Enterprise_Name_of_skill_Group. Also note that the names of the labels are case sensitive.

6. On the Network Target tab, provide the following details:
   - Target type (filter): From the dropdown list, select Network VRU.
   - Network Target: Select the Network VRU configured for Unified WIM and EIM (page 24).

   Click Save.

![Configure the label]

Configuring Script Selectors

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

Individual script selectors are required for the following activities: inbound email, outbound email, chat, callback, and delayed callback activities. Make sure to complete these steps for each type of activity.

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.
5. In the Dialed Number/ Script Selector section, click Add.
A new entry is created and the Attributes tab becomes editable.

6. On the Attributes tab, provide the following details:
   - **Routing client:** From the dropdown list, select the routing client configured for the MR PG in step 9 in “Configuring Media Routing Peripheral Gateways (MR PGs)” on page 26.
   - **Media routing domain:** From the dropdown list, select the MRD configured for Unified EIM and WIM (page 22).
   - **Name:** Provide a name for the script selector.
   - **Default label:** Select the label configured for Non-IPTA skill groups (page 41). This needs to be set up only for script selectors for inbound email, outbound email, and chat activities.

7. Click the Dialed Number Mapping tab. Click **Add**.

8. On the Dialed Number Map Entry window, associate the script selector with a call type.
9. Click **OK** to save the entry. Then click **Save** to save the script selector configuration.

## Creating Scripts

A routing script determines the path and target object for an activity routed from Unified EIM and WIM to Unified CCE. Individual routing scripts are required for the following activities: inbound email, chat, callback, and delayed callback activities. Make sure to complete these steps for all these activities. You do not need routing scripts for outbound email activities.


The following procedure shows how to set up a particular script. To find out more about setting up different types of scripts to meet your routing requirements, see the *Scripting and Media Routing Guide* for Unified CCE.

### To create 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 Start node is added by default to the script editor.

4. In the Script Editor window, go to View > Palette.

The Palette window opens.

5. In the Palette window, on the Queue tab, click the **Queue** button, and click in the script editor. The Queue to Skill Group node is added to the script editor.

6. Double-click the Queue to Skill Group node to open the Queue to Skill Group Properties window.
7. In the Queue to Skill Group Properties window, on the Queue tab, in the Skill Group column, select an IPTA skill group.

Select an IPTA skill group

8. Next, in the Palette window, on the Targets tab, click the Label button, and click in the script editor. The Label node is added to the script editor.

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

10. 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.

Select the label type and a label
11. Next, in the Palette window, 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.

12. Click the **Validate Script** button to check if the script is created properly. If there are any errors, fix them.

13. Click the **Save** button to save the script.

A sample script

To display dynamic content (page 62) to chat customers (for example, wait time, activity ID, etc.) while chat requests are being processed by the system, ensure that the Run External Script node is configured.

14. In the ICM script, add the Run External Script node and select the Network VRU script created on page 24.
The script will look like this.

A sample script

After creating a script, map the script to a call type, MRD, and script selector. Also set the run schedule for the script.

15. In the Script Editor window, go to **Script > Call Type Manager**.

16. In the Call Type Manager window, in the Call Directory tab, do the following:
   a. In the Media Routing Domain field, from the dropdown list, select the MRD configured for Unified EIM and WIM (page 22).
   b. In the Script Type Selector field, from the dropdown list, select the script selector created for the MRD (page 42).
c. Next, click the **Add** button. The Add Call Type Selector Entry window appears. In the Call type field, select the call type configured for Unified WIM and EIM (page 25). Click **OK**.

![Add Call Type Selector Entry window](image)

*Map the script to a call type, MRD, and script selector*

17. In the Call Type Manager window, in the Schedule tab, do the following:
   a. In the Call type field, from the dropdown list, select the same call type you selected in Step 16.
   b. Next, click the **Add** button. In the Add Call Type Schedule window that appears, do the following:
      i. In the Script tab, select the script configured for Unified WIM and EIM (page 44).
      ii. In the Period tab, set a schedule for the script.
      iii. Click OK.

![Add Call Type Schedule window](image)

*Set a schedule for the script*

18. Click **OK** to close the Call Type Manager window.
Configuring Device Targets

Individual device targets are required for routing voice calls for callback and delayed callback activities. Complete these steps for all these activities. Device targets are not needed for inbound email, outbound email, and chat activities.

To configure a device target:

1. Go to **Start > All Programs > ICM Admin Workstation > Configuration Manager**.
2. In the Configuration Manager window, browse to **Tools > Explorer Tools > Device Target Explorer**.
3. Double-click **Device Target Explorer**.
4. In the Device Target Explorer window, click **Add Device Target**.
5. Provide the name and global address, which is the host name of the Unified CCE server followed by the agent extension, in the following format: *Unified_CCE_Server* Agent_Extension.
6. Provide the configuration parameter in the following format. The string before the agent extension must be exactly as specified: */devtype CiscoPhone/dn Agent_Extension*
7. Click the **Add Label** button.
   The Label tab appears.
8. On the Label tab, set the following:
   - **Routing client**: From the dropdown list, select the MR PG configured for Unified WIM and EIM (page 26).
   - **Label**: Provide the name of the label. The label name must be the *Agent_Extension*.
9. Click **Save**.
Configuring Expanded Call Context (ECC) Variables

ECC variables are used in Unified CCE scripts to facilitate and influence routing. ECC variables have a maximum length of 256 characters. Both Scalar and Array ECC variables are supported.

ECC variables are required for inbound email, outbound email, chat, callback, and delayed callback activities. Create the following ECC variables:

- For inbound and outbound email activities: `user.cim.activity.id`
- For chat activities: `user.cim.activity.id`, `user.wim.customer.name`
- For callback and delayed callback activities: `user.cim.activity.id`, `user.wim.customer.name`, `user.cisco.cmb`, `user.cisco.cmb.callclass`

To configure an ECC variable:

1. Go to Start > All Programs > ICM Admin Workstation > Configuration Manager.
2. In the Configuration Manager window, browse to Tools > Miscellaneous Tools > System Information.
3. In the System Information window, in the General section, select the Expanded call context enabled option. Click Save.
4. In the Configuration Manager window, browse to Tools > List Tools > Expanded Call Variable List.
5. Double-click Expanded Call Variable List.
6. In the Expanded Call Variable List window, in the Select filter data section, click Retrieve. Then, in the Expanded Call Variable section, click the Add button.
7. Type the name and length of the ECC variable. A maximum of 256 characters are allowed. Make sure to use the exact names as provided here.
   - `user.cim.activity.id` (needed for all types of activities)
Preparing Unified CCE for the Integration

- `user.wim.customer.name` (needed for chat, callback, and delayed callback activities)
- `user.cisco.cmb` (needed for callback and delayed callback activities)
- `user.cisco.cmb.callclass` (needed for callback and delayed callback activities)

8. Click Save.

Configure ECC variables

---

**Installing Cisco Media Blender**

- Ensure that Cisco Media Blender (CMB) is installed and configured with Unified CCE. It is required for callback and delayed callback activities. For details, refer to the *Cisco Media Blender Installation Guide for Cisco Unified Contact Center Enterprise & Hosted Editions*.

---

**Installing Unified EIM and WIM and the Integration**

For details about performing the tasks mentioned in this section, see the *Cisco Unified Web and E-Mail Interaction Manager Installation Guide*.

**To install Unified EIM and WIM and the integration with Unified CCE:**

1. Ensure that Microsoft SQL Server 2008 R2 is installed and running on the machine on which the Unified EIM and WIM databases will be installed.
2. From the Unified EIM and WIM Environment CD, copy the JBoss folder to a local directory on the Unified EIM and WIM messaging server and all application servers.
3. From the JBoss folder inside the local directory, extract the files from the jboss-as-7.1.2.Final.zip file to the location where JBoss is to be installed.

4. In distributed-server installations, install JDK 1.7 Update 2 or higher (64-bit) on all machines where the services server, messaging server, and application servers are to be installed. The installation program for JDK 1.7 Update 7 is included in the Environment folder of the installation package.

5. On the web server machines, install Microsoft IIS.

6. Install Unified EIM and WIM. Refer to the *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 Cisco Interaction Manager with Unified CCE.”


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

9. On the user desktops, install Sun JRE 1.6.0 (Update 30 or higher). Version 1.6.0_30 is included on the product CD.

10. 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 the System for Multiple Agent PGs

Multiple Agent PGs can be used for Unified CCE installations. A maximum of four Agent PGs are supported for each deployment of Unified EIM and WIM. Note that a unique application path and associated application path members are needed for each Agent PG. The application path is used by the Listener Service to connect and communicate with the Agent PG.

**To configure the system for multiple Agent PGs:**

1. Create the Agent PGs. For Unified CCE installations, see page 31.

2. In Unified CCE, configure agents ([page 36](#)) and skill groups ([page 37](#)).

3. Run the Cisco Interaction Manager Integration Wizard to import the Agent PGs. For each Agent PG that is imported, a Listener instance is created in the System Console. Refer to the *Cisco Unified Web and E-Mail Interaction Manager Integration Guide for Unified CCE* for details about running the wizard.

4. Log in to the Cisco Integration Manager System Console.

5. Browse to **Shared Resource** > **Services** > **Listener** > **Listener**. In the List pane, select the Listener process. In the Properties pane, in the **Maximum number of instances** field set the value as 4.

6. Browse to **Partitions** > **Partition**. In the Properties pane, on the Services tab, set the number of instances for the Listener service to 4.

   For details about steps 4-6, see the *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to System Console*.  

---

52  Cisco Unified Web and E-Mail Interaction Manager Deployment and Maintenance Guide
Configuring Finesse

Cisco Finesse enables the use of custom gadgets for Voice & Multichannel (Unified EIM and WIM), facilitating the Unified EIM and WIM user interface to be embedded within a gadget to provide contact center agents a unified desktop experience.

---

**Important:** Before you begin the configuration, ensure that the Finesse VM and software are installed and ready for use.

---

Configuring Finesse Files

Perform these tasks from any local machine.

**To configure the eim_wim_server_url.js file:**

1. Copy the contents of the Finesse folder from the installation DVD to a temporary directory, Temp, on your local machine.
2. From the Temp/Finesse folder open the eim_wim_server_url.js file in a text editor.
3. Locate the following text in the file:

   ```javascript
   var eim_wim_server_url =
   "http://<Load_Balancer_or_Web_Server_Host_Name>/<Context_Root_Name>/web/view/platform/common/login/top.jsp?partitionId=1";
   ```

   Replace `<Load_Balancer_or_Web_Server_Host_Name>` with the host name of the Unified EIM and WIM web server. If the deployment uses a load balancer, provide the host name of the load balancer.

   Replace `<Context_Root_Name>` with the context root name defined for the application at the time of installing Unified EIM and WIM.

   If the Unified EIM and WIM installation is configured with SSL, replace `http` with `https`.

Enabling 3rdpartygadgets Account and Deploying the Gadget

Perform these tasks on the Finesse server.

**To enable the 3rdpartygadgets account and deploy the Gadget:**

1. Using the Finesse Console, login as an administrator and enable the 3rdpartygadgets account on the Finesse server.

   When you enable the 3rdpartygadgets account, a files folder gets created automatically.

2. Create a new folder called CIM under the files folder.

3. Deploy the gadget files from the Temp/Finesse folder on your local machine (page 53) to the Finesse server using a secure FTP client.

4. Start the Cisco Tomcat service on the Finesse Server.
Configuring Finesse Settings and Layout

Perform these tasks from any local machine.

To configure the Finesse settings and layout:

1. Launch the URL: http://Finesse_Server_Name/cfadmin. Login as a finesse administrator.

2. Configure the Contact Center CTI Server Settings and Contact Center Enterprise Administration & Data Server Settings.

3. Configure the Layout. In the Finesse Layout XML, add the following code:

```xml
<tab>
    <id>TD</id>
    <label>Label_Name</label>
    <gadgets>
        <gadget>http://localhost/3rdpartygadget/files/CIM/CIM.xml</gadget>
    </gadgets>
</tab>
```

Where:
- *ID*: Provide an ID for the new gadget. Make sure that the ID name does not have any spaces. For example, UnifiedEmailandWebInteractionManager.
Label_Name: Provide a label for the gadget. For example, Unified Email and Web Interaction Manager.

Starting Finesse Services

To start the Finesse services:

On the Finesse server, restart Finesse Services by doing the following:

1. Connect to the Finesse Server using a remote client tool. For example, putty.
2. Login using the Finesse Administrator account.
   
   `utils service stop Cisco Tomcat`

   
   `utils service start Cisco Tomcat`
Setting Up Integrated Objects

- Configuring Variables in Unified EIM and WIM
- Verifying Mapping of Objects in the Administration Console
- Setting Up Knowledge Base Articles for Unified EIM
- Setting up Business Objects in the Administration Console
- Setting Up Services in the System Console
- Setting Up Web Links for Chat and Collaboration
- Configuring Dynamic Messages for Integrated Chats
- Handling Email Assignment
- Related Documentation
This chapter provides an overview of the process of setting up Unified WIM and EIM–Unified CCE objects.

## Configuring Variables in Unified EIM and WIM

While sending new activity requests from a queue to Unified CCE, EAAS sends call variables and ECC variables to Unified CCE as task context. By default, the following activity attributes are sent to Unified CCE as ECC variables.

- For inbound and outbound email activities: activity_id
- For chat activities: activity_id, customer_name
- For callback and delayed callback activities: activity_id, customer_name, cmb_param, cti_strategy

If you need to pass on other attributes of the activity as call variables or ECC variables to Unified CCE, you need to configure them in Unified EIM and WIM. These variables can then be used in Unified CCE scripts to configure conditions. For details, see the Unified CCE scripts documentation. If you plan to configure these variables as ECC variables in Unified EIM and WIM, you need to first create the ECC variables in Unified CCE. For details, see the Unified CCE documentation.

You can also create variables for custom activity attributes. For details about creating variables, see the “Call Variables” chapter in the *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Routing and Workflows.*

## Verifying Mapping of Objects in the Administration Console

To verify that Unified CCE objects have been mapped correctly in the Unified EIM and WIM Administration Console:

2. Log in as the partition administrator (user name and password that were configured during the installation of Unified EIM and WIM). Go to the Administration Console.
3. 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. For details, see the *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Administration Console.*
4. Under the appropriate department, browse to the **User > Users** node in the Administration tree, to verify that all users mapping to the administrators, supervisors, and agents, which were selected at the time of running the integration wizard, are displayed. Note that after the integration wizard is run, additional mapped users can be created from the Administration Console. For details, see the *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Administration Console.*
5. Under the appropriate department, click the User > Groups node in the Administration tree to verify that all user groups mapping to the skill groups, which were selected at the time of running the integration wizard, are displayed. Note that after the integration wizard is run, additional mapped user groups can be created from the Administration Console. For details, see the Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Administration Console.

6. Under the appropriate department, click the Workflow > Queues node in the Administration tree, and verify that all queues mapping to the MRDs, which were selected at the time of running the Unified CCE integration wizard, are displayed. Also verify that for all the non-IPTA skill groups that were imported using the Unified CCE integration wizard, the corresponding queues have been automatically created under the Queues node. Note that after the integration wizard is run, additional mapped queues can be created from the Administration Console. For details, see the Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Routing and Workflows.

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 the Cisco Unified Web and E-Mail Interaction Manager Knowledge Base Author’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 Departments > Department_Name > Content > 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.
5. Browse to the Department > Shared folder. 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.

This article will be used later in a workflow (see page 59).
Setting up Business Objects in the Administration Console

Unified EIM Objects

See the Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Email Resources and the Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Routing and Workflows for the details of the procedures mentioned in this section.

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

2. Log in as the partition administrator and go to the Administration Console.
3. In the Administration tree, browse to the Administration > Departments > Department_Name > Classifications > Categories node. Create categories. These categories will be used later in a workflow (see page 59).
4. Now, browse to the Email > Aliases node. Create an alias to serve as the entry point for emails into the system.
5. Next, browse to the Workflow > Queues node to create an email queue. Skip this step if you want to use an auto-configured queue (see page 58).
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 the auto-configured queues or use the queues created in Step 5 to the Queue node. Select the auto-acknowledgement KB article created earlier (see page 58) for the Auto-acknowledgement node. Select the categories created in Step 3 for the Classifications node.

Unified WIM Objects


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

2. Log in as the partition administrator and go to the Administration Console.
3. Browse to the Workflow > Queues node and create chat, callback, and delayed callback queues. Skip this step if you want to use auto-configured queues (see page 58).
4. Browse to the Chat > Entry points node. Create new entry points by assigning the appropriate templates. To route chats and call back activities that enter from this entry point, use an auto-configured queue or the queue created in Step 3. Make the entry points active. The configuration steps for entry points are different for different types of activities and routing options.
   - The activity types for which you need to create entry points are: Chat, Callback, Delayed callback. The two routing options available are: Cisco Interaction Manager and Unified CCE.
5. 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 *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Chat and Collaboration Resources*.

### 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 Administrator’s Guide to System Console* 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 Cache**: Maintains the files that store information about objects used in workflows.
- **Workflow Engine**: Applies workflows on emails to automate their routing and handling.
- **Dispatcher**: Sends outgoing emails out of the system.
- **External Agent Assignment Service (EAAS)**: Identifies new activities that arrive into an external assignment queue, and routes requests for each of these activities to Unified CCE for routing to take place through Unified CCE.
- **Listener**: Assigns activities to target agents or user groups (skill groups) identified by Unified CCE, and reports the status of both the activity and the agent to Unified CCE throughout the life cycle of the given activity.

### To set up Unified EIM services in the System Console:

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

1. Open a new browser window, and launch the URL: `http://Unified EIM and WIM_Server/Context_Root`. Log in as the system administrator (user name and password that were configured during the installation of Unified EIM and WIM). Go to the System Console.

2. Browse to the **Partitions > Partition > Services > Email > 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 59).

3. 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. Also ensure that the start type for the service process is set to automatic.

4. Navigate back to the **Partitions > Partition > Services > Retriever** node. Ensure that the start type for the service instance is set to automatic. Stop and start the Retriever instance.
5. Browse to Shared Resource > Services > Workflow > Workflow Cache and verify that the Workflow Cache process is running. If the process is in a stopped state, start the process by clicking the Run button. Also ensure that the start type for the service process is set to automatic.

6. Browse to Partitions > Partition > Services > Workflow > Workflow Cache and ensure that the start type for the service instance is set to automatic. Start the Workflow Cache instance.

7. 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. Also ensure that the start type for the service process is set to automatic.

8. Browse to Partitions > Partition > Services > Workflow > Workflow Engine and ensure that the start type for the service instance is set to automatic. Start the Workflow Engine instance.

9. 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. Also ensure that the start type for the service process is set to automatic.

10. Browse to Partitions > Partition > Services > Email > Dispatcher and ensure that the start type for the service instance is set to automatic. Start the Dispatcher instance.

11. 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. Also ensure that the start type for the service process is set to automatic.

12. Browse to Partitions > Partition > Services > Listener > Listener. Verify that the Listener instance for the Agent PG is automatically created. Also ensure that the start type for the instance is set to automatic. Then start the Listener instance.

13. 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. Also ensure that the start type for the service process is set to automatic.

14. Browse to Partitions > Partition > Services > EAAS > EAAS. Configure the EAAS instance by providing the MR Connection port number you provided while creating the MR PIM (page 26). Also ensure that the start type for the instance is set to automatic. 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 services:

- **External Agent Assignment Service (EAAS):** Identifies new activities that arrive into an external assignment queue, and routes requests for each of these activities to Unified CCE for routing to take place through Unified CCE.

- **Listener:** Assigns activities to target agents or user groups (skill groups) identified by Unified CCE, and reports the status of both the activity and the agent to Unified CCE throughout the life cycle of the given activity.

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

- Follow the instructions in steps 11-14 in “Unified EIM Services” on page 60.
Setting Up Web Links for Chat and Collaboration

To create a chat and collaboration link on your web site:

- Open the code view of the host web page and add the edited link code (see page 59) 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.

Configuring Dynamic Messages for Integrated Chats

Dynamic Run Application Script Request (DRASR) allows you to display wait messages with dynamic text (such as expected wait time) to customers while chat and call requests are being processed by the Unified WIM and Unified CCE integrated systems. You can use ECC variables and call variables to display the dynamic content. The dynamic messages are configured in the egicm_message_map.xml file. This file is available in the ipcc folder in the configuration.zip file available on the services server at the following location: 

`Cisco_Home\eService\lib`

Configuring the dynamic messages includes the following steps:

1. Configure the Network VRU scripts in Unified CCE.
2. Identify the queues for which you want to display the dynamic messages.
3. Identify the ECC variables or call variables you want to use in the dynamic message and prepare the macros for the variables. For details about these objects and how they are used in Unified CCE, see the Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted available here: [http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)
4. Configure the dynamic message in the egicm_message_map.xml file.

Dynamic messages can be displayed for integrated chats, callback, and delayed callback activities.

To configure dynamic messages for integrated chats:

1. From Unified CCE, configure the Network VRU scripts (page 24) and use them in the ICM scripts (page 44) used for chat activities. You will need the name of the Network VRU script for configuring the dynamic messages.
2. From the Unified EIM and WIM Administration Console, identify the integrated chat queues for which you want to display the dynamic messages.
3. To display the dynamic content using ECC variable macros, prepare your macros by doing the following:
   a. Look at the “Configuring Variables in Unified EIM and WIM” on page 57 section for the names of ECC variables that can be used.
b. Identify the ECC variables you want to use in the message. The macro will be added in the format `%ECC <Variable_Name>%`. For example, `%ECCuser.cim.activity.id%`.

**Important:** While selecting ECC variables to be used in macros, make sure that the variables have valid values. If you use a variable that does not have a value, a run application script failure will occur and the customer will not be able to chat. The error template is displayed to the customer.

4. To display the dynamic content using call variable macros, prepare your macros by doing the following:

- From the Administration Console, from the Call Variables tab of the queue properties (page 62), identify the call variables you want to use in the message and note down the number associated with the call variable. For example, in the following figure the number for `customer_phone_no` is 1 and for `activity_id`, the number is 2. The macro is added in the format `%CV(Number)%`. For example, `%CV1%` for `customer_phone_no`.

**Order of call variables**

5. On the Cisco Interaction Manager services server, extract the `egicm_message_map.xml` file from the `ipcc` folder in the `configuration.zip` file available at: `Cisco_Home\eService\lib`.

6. Open the `egicm_message_map.xml` file in a text editor.

7. In the file, locate the `<MESSAGE_MAPPINGS>` line and add the following line under it.

```
<Script_Name isURL="yes/no" isViewPort="yes/no">Message</Script_Name>
```

Where:

- **Script_Name**: Name of the Network VRU script (page 24). The name you provide in the XML file should exactly match the name provided while configuring the Network VRU script.
- **isURL**: Set the value to `yes` if you are using a URL in the message and you want to open the URL on the customer side. When the value is set to `yes`, the complete message is considered as a URL by the system. In such cases, only provide the URL in the message and do not provide any text.
**isViewPort:** Set the value to `yes` to open the web page sent as part of the message in a new window. If you want the web page to open in the Chat Customer Console, set the value as `no`.

**Message:** The message you want to display to customers. The message can include dynamic variables (ECC variable (Step 3) and call variable (Step 4)). These macros are parsed at runtime and are displayed to the customers in the Chat Customer Console. The symbol “%” should be used only for adding macros to the message. If it is used otherwise, a run application script failure will occur and the customer will not be able to chat. The error template is displayed to the customer. If you are using a URL in the message, make sure you provide the complete URL and not a relative URL. For example, `http://www.CompanyName.com/`. When the `isURL` property is set to `yes`, the complete message is considered as a URL by the system. In such cases, only provide the URL in the message and do not provide any text.

The new line can look like:

```xml
<CIMExternalApplicationScript isURL="no" isViewPort="no">An agent is expected to be available in approximately %ECCwait.time% minutes. While you are waiting, checkout the latest offers on our website. </CIMExternalApplicationScript>
```

If you are opening a web page in a new window, the line will look like:

```xml
<CIMExternalApplicationScript isURL="yes" isViewPort="yes">http://www.CompanyName.com/offers</CIMExternalApplicationScript>
```

---

8. Add the updated `egicm_message_map.xml` file to the `ipcc` folder in the `configuration.zip` file available at the following location on the services server: `Cisco_Home\eService\lib`

9. Restart the Cisco service on the application, messaging, and services servers in the Unified EIM and WIM installation for the changes to take effect.
Handling Email Assignment

After activities are processed by Unified EIM, EAAS changes the activity substatus to 4105 (Ready for Unified CCE routing) and sends a request to Unified CCE for further processing. If the same activities continue to remain in this substatus for a delayed period, various options exist to have EAAS retry routing of such activities through Unified CCE. The options available are:

- **Option 1:** A maximum wait time for each mapped queue can be set. When an activity belonging to that queue reaches that time, and it has not been assigned to an agent or to an exception queue, EAAS requeues the activity again and sends a **NEW_TASK** request for that activity to MR PIM.
- **Option 2:** This option can only be used when Unified CCE scripts are linear in nature. When an activity is picked for assignment, EAAS checks to see if there are any activities older than the currently picked activity that are not yet assigned to an agent or to the exception queue. If any such activities are found, EAAS requeues those activities again and send a **NEW_TASK** requests for them to MR PIM.

**To enable option 1:**

1. On the Unified EIM active database, run the following query to get the queue_ID of integrated email queues.

   ```sql
   SELECT queue_ID, queue_name FROM EGPL_ROUTING_QUEUE
   ```

2. For each integrated email queue, run the following query to set the **MAX_WAIT_TIME** column value in seconds. This should be the maximum time in which you want MR PIM to respond back to a **NEW_TASK** request.

   ```sql
   UPDATE EGICM_QUEUE SET MAX_WAIT_TIME = Value in seconds WHERE QUEUE_ID = Queue_ID of Integrated email queue
   ```

**To enable option 2:**

- Run the following query on the Unified EIM active database to change the value of the setting **FIFO_ALGO_TO_SAVE_EMAIL_ENABLE** to True.

  ```sql
  Update egpl_config_property set Value='true' where domain='ipcc.egicm_configuration.properties' and NAME = 'FIFO_ALGO_TO_SAVE_EMAIL_ENABLE'
  ```

Related Documentation

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

- *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Administration Console* helps administrators set up and manage business objects.
- *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Email Resources* helps administrators set up aliases, blocked addresses, delivery exceptions, and blocked file extensions.
- *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Routing and Workflows* helps administrators set up service levels, queues, and workflows.
- *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Data Adapters* helps administrators set up data links to connect to external sources.

- *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to System Console* helps system administrators set up and manage services, loggers, and system monitors.

- *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Tools Console* 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.

- *Cisco Unified Web and E-Mail Interaction Manager Supervisor’s Guide* helps supervisors set up and use agent and queue monitors.

- *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Reports Console* helps managers and supervisors to set up and run reports to analyze various aspects of the system.

- *Cisco Unified Web and E-Mail Interaction Manager Knowledge Base Author’s Guide* helps knowledge base (KB) managers and authors to create and publish KB articles.

Managing and Maintaining Servers

- Encrypting SQL Server Database
- Best Practices for Configuring Servers
- Routine Maintenance Tasks
- Performance Tuning Considerations
Encrypting SQL Server Database

Perform these tasks after the Unified EIM and WIM installation is complete.

1. Create a master key in the master database. This key is then used to create the server certificate that can be used to secure the database encryption key. Connect to the master database and run the following query.

   ```sql
   USE master
   GO
   CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'company@123'
   GO
   ```

2. Backup the master key. This creates a certificate in the master database.

   ```sql
   BACKUP MASTER KEY TO FILE = 'c:\temp\masterkey'
   ENCRYPTION BY PASSWORD = 'company@123'
   GO
   ```

3. Now create the server certificate database encryption key ("DEK").

   ```sql
   USE master
   GO
   CREATE CERTIFICATE DEKCert WITH SUBJECT = 'DEK Certificate'
   GO
   ```

4. Create a backup of the server certificate database encryption key ("DEK").

   ```sql
   BACKUP CERTIFICATE DEKCert TO FILE = 'c:\DEKCert'
   WITH PRIVATE KEY ( FILE = 'c:\temp\DEKCertPrivKey',
   ENCRYPTION BY PASSWORD = 'company@123' )
   GO
   ```

5. Create database encryption key for the database where you wish to configure transparent data encryption. In the following query, `eGActiveDB_name` is the name of the active database.

   ```sql
   USE eGActiveDB_name
   GO
   CREATE DATABASE ENCRYPTION KEY
   WITH ALGORITHM = AES_128
   ENCRYPTION BY SERVER CERTIFICATE DEKCert
   GO
   ```

You now have all the prerequisites for enabling transparent data encryption, so database encryption can be enabled.

6. Enable database encryption. Run the following query where `eGActiveDB_name` is the name of the active database.

   ```sql
   ```
ALTER DATABASE $ActiveDB_name$ SET ENCRYPTION ON

By setting encryption on, a background task starts encrypting all the data pages and the log file. This can take a considerable amount of time, depending on the size of the database.

Database maintenance operations should not be performed when this encryption scan is running.

7. To query the status of the database encryption and its percentage completion, query the new sys.dm_database_encryption_keys DMV:

SELECT DB_NAME(e.database_id) AS DatabaseName,
    e.database_id,
    e.encryption_state,
    CASE e.encryption_state
        WHEN 0 THEN 'No database encryption key present, no encryption'
        WHEN 1 THEN 'Unencrypted'
        WHEN 2 THEN 'Encryption in progress'
        WHEN 3 THEN 'Encrypted'
        WHEN 4 THEN 'Key change in progress'
        WHEN 5 THEN 'Decryption in progress'
    END AS encryption_state_desc,
    c.name,
    e.percent_complete
FROM sys.dm_database_encryption_keys AS e
    LEFT JOIN master.sys.certificates AS c
    ON e.encryptor_thumbprint = c.thumbprint

---

Best Practices for Configuring Servers

For All Servers

This section describes the best practices for configuring all the Unified EIM and WIM servers. For database server, there are some additional best practices that are listed in the section “Additional Best Practices for Database Servers” on page 70.

Allocating Adequate Virtual Memory

- Virtual memory setting should be set to 1.5 times the physical memory. To ensure that adequate space is available during run time, distribute the virtual memory across disk volumes.
**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**

- To ensure that virus and malware scanning software on the servers do not interfere with the performance of the application, certain folders and files must be excluded from continuous virus scanning. Since no files are downloaded to these locations from the internet, it is safe to exclude these directories from virus scanning. For details about doing this task, see the “Post-Installation Tasks” chapter in the *Cisco Unified Web and E-Mail Interaction Manager Installation Guide*.

**Additional Best Practices for Database Servers**

In addition to the best practices that apply to all the Unified EIM and WIM servers, there are some special best practices for the database server that are described in this section.

**Installation and Settings**

- If you are using RAID configuration, ensure that the RAID strip size is set to 64 kilobytes for SQL Server data and log file array.

- Ensure that the Data and Log drive array is formatted as NTFS with 64 kilobytes in each allocation unit.

- Check the values set for **fill factor** and **max degree of parallelism**. To reduce I/O (disk input output) on SQL server, the fill factor should be set to 80%. This ensures that 20% free space is available in the data pages of indexes, and it reduces page splitting. The max degree of parallelism should be set to the number of physical processors. For example, if there are two processors, set *max degree of parallelism* to 2; and if there are five processors, set *max degree of parallelism* to 5.

  a. On the database server, run the following stored procedure.

     ```
     EXEC sp_configure 'show advanced option', '1'
     Reconfigure
     exec sp_configure
     ```

  b. If the fill factor and max degree of parallelism is not configured correctly, run the following stored procedure on the database.

     ```
     exec sp_configure 'fill factor (%)', 80
     exec sp_configure 'max degree of parallelism', Number_Of_Physical_Processors
     reconfigure with override
     ```

- In order to ensure that select queries from the application execute optimally, and with the least possibility of encountering SQL deadlocks with other modification queries, it is required that the **Read commit snapshot** property is enabled for the Active database. To enable this property:

  a. Ensure that Unified EIM and WIM is stopped completely. All distributed components such as the services server, all application servers and messaging server should be stopped. For these commands to succeed, there must not be any database connections to the *ActiveDB*. 

---

70  Cisco Unified Web and E-Mail Interaction Manager Deployment and Maintenance Guide
b. Verify the current value of the **Read commit snapshot** property for the Active database by running the following select query:

```sql
select name, snapshot_isolation_state_desc, is_read_committed_snapshot_on from sys.databases
```

c. If the **Read commit snapshot** property is disabled, run the following query to enable it:

```sql
alter database Active_Database_Name set single_user with rollback immediate;
alter database Active_Database_Name set read_committed_snapshot on;
alter database Active_Database_Name set multi_user;
```

d. Verify that the **Read commit snapshot** property has been enabled successfully by running the following query.

```sql
select name, snapshot_isolation_state_desc, is_read_committed_snapshot_on from sys.databases
```

**Temp Database**

- Set the temp database properties as follows:
  - Data file size should be set to 1.5 GB. Autogrowth should be set to 1 GB.
  - Transaction log file size should be set to 1 GB. Autogrowth should be set to 1 GB.

**Master Database**

- Set the master database properties as follows:
  - Data file size should be set to 50 MB. Autogrowth should be set to 50 MB.
  - Transaction log file size should be set to 50 MB. Autogrowth should be set to 50 MB.

**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. To calculate the required free disk space, see the *Cisco Unified Web and E-Mail Interaction Manager Solutions Reference Network Design Guide*.

- Set the active database properties as follows:
  - Data file size should be set to 20 GB. Autogrowth should be set to 1 GB.
  - Transaction log file size should be set to 2 GB. Autogrowth should be set to 1 GB.

**Archive Database**

- **Important:** The Archive database is available only in installations that use the Standard Edition of Microsoft SQL.

- Set the archive database properties as follows:
  - Properties of Datafile: Data file size should be set to 5 GB. Autogrowth should be set to 500 MB.
  - Transaction log file size should be set to 2 GB. Autogrowth should be set to 2 GB.
Reports Database

Important: The Reports database is available only in installations that use the Enterprise Edition of Microsoft SQL.

- Set the reports database properties as follows:
  - Data file size should be set to 20 GB. Autogrowth should be set to 1 GB.
  - Transaction log file size should be set to 2 GB. Autogrowth should be set to 1 GB.

Optimal Configuration Settings

The following table describes optimal settings for the databases.

<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>
<tr>
<td>torn_page_detection</td>
<td>on</td>
</tr>
<tr>
<td>database auto grow</td>
<td>on</td>
</tr>
<tr>
<td>transaction log auto grow</td>
<td>on</td>
</tr>
</tbody>
</table>

To configure the settings:

1. Run the following query on the Cisco Interaction Manager databases to set the values for the auto close, auto create statistics, auto update statistics, auto shrink, torn page detection, and read write properties:

   ```sql
   alter database Database_Name
   set auto_close on, auto_create_statistics on, auto_update_statistics on,
   auto_shrink off, torn_page_detection on, read_write
   ```

2. Do the following steps to configure the database auto growth and transaction log auto growth settings.
   a. In the Microsoft SQL Server Management Studio, browse to Databases > Database_Name.
   b. Right-click the database name and from the menu, select Properties. In the Database Properties window select Files, and in the Database files section, in the Autogrowth field click the Assistance button.
c. In the Change Autogrowth for File_Name window, select the **Enable Autogrowth** setting and configure the autogrowth settings.

![Enable the autogrowth setting](image)

---

**Routine Maintenance Tasks**

**For All Servers**

This section describes the routine maintenance tasks for the Unified EIM and WIM servers. For database server, there are some additional tasks that are listed in the section “Additional Tasks for Database Servers” on page 74.

**Monitoring Disk Space**

- Monitor and free space on disk volumes periodically by deleting the unnecessary files. Installation programs, application logs, user profiles, Dr. Watson logs, temp files are known to occupy the space unnecessarily. It is recommended that such files are deleted on a regular basis. 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**

- Apply the security patches released by Microsoft to plug vulnerabilities in the operating system and various programs.

**Creating Backup Copies**

- Back up the *Cisco_Home* folder on the file, application, messaging, and services servers regularly. Exclude the *log* folder under *Cisco_Home* from the backup. The process of backing up the database is different. For details, see the section “Additional Tasks for Database Servers” on page 74.
Additional Tasks for Database Servers

In addition to the routine maintenance tasks that apply to all the Unified EIM and WIM servers, there are some special tasks for the database server that are described in this section.

Performing Disk Defragmentation

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

Monitoring Summarization Job Runs

On a weekly basis, verify that all the summarization jobs enabled for Unified EIM and WIM are running successfully at the scheduled times.

To view the summarization job run details:

1. In the Microsoft SQL Server Management Studio, browse to SQL Server Agent > Jobs.
2. In the jobs list, locate the job `populatesmy_Database_Name`. Where `Database_Name` is the name of the active database (in SQL Server Standard installations), or the reports database (in SQL Server Enterprise installations).
3. Right-click the `populatesmy_Database_Name` job and from the menu select View History.
4. In the Log File Viewer window, browse to Job History and check the following:
   - In the Date column, the date and time should not be very old as jobs run every 30 minutes.
   - For all successfully run jobs, the date column will show a green check mark.
The jobs that did not run successfully, will show a warning sign and you can expand the row to see the reason of failure.

Sample job runs

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 transactional logs growing indefinitely.

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

Archiving

**Important:** The Archive database is available only in installations that use the Standard Edition of Microsoft SQL.

Regular archiving helps to keep the size of the database manageable. The maximum size of the active database must be kept under 110 GB.

- Schedule archive jobs to run during off-peak hours to avoid database performance bottlenecks.
- Purge archived activities to create more available disk space.
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 to plan the configuration when you first set it up. In this section, we provide a quick overview of some of the factors that should be considered 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.

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.
Modifying the Unified EIM and WIM EAR

- About the PackIt Utility
- Configuring the Utility
- How To
To make changes to the installation files, you must use the PackIt Utility. This chapter provides an overview on what this utility allows you to do, and how to use it.

### About the PackIt Utility

Some of the changes in the product, like creating custom rules and conditions for workflows, require updating the EAR and some configuration and JAR files on the services server. The PackIt utility provides a user interface to make such changes to the files easily. Using this utility you can:

- Add third party JARs in EAR for customizations.
- Add schema and query files in the `configuration_custom.zip` file in the EAR.
- Add or update custom classes in `egpl_custom.jar`.
- Add new Java Data Adapter implementation classes in the EAR.
- Add or update custom rules and conditions for workflows.
- Add or update connection pool information for databases.

### Configuring the Utility

Utility is available on the services server in the `Cisco_Home\Utilities\egainpackit` folder.

The ear should always be picked from the file server from the `Cisco_Home\eService\installation\ear` folder. Customers should make sure that the version on the file server is the latest one.

The utility can be run on any desktop. The desktop needs to have JDK 1.7 Update 2 or higher installed on the machine.

**To configure the utility:**

1. Copy the contents of the following folder from the services server on the machine where you want to run the utility: `Cisco_Home\Utilities\egainpackit`
2. Open the \texttt{egainpackit.bat} file in a text editor. Locate the \texttt{SET JAVA_HOME} property and set the value to the location where JDK 1.7 Update 2 or higher is installed on your machine. For example, \texttt{C:/Java/jdk1.7.0_02}. Double-click \texttt{egainpackit.bat} to launch the utility.

\textit{The PackIt utility}

\textbf{How To}

This section describes how to:

- Add New Custom Rules to be used in WorkFlows
- Add New Custom Conditions to be used in WorkFlows
Add New Connection Pools for SQL JDBC Data Adapters
Update Connection Pools for SQL JDBC Data Adapters
Remove a Redundant Connection Pool
Extract Connection Pool File egpl_ds_connpool_map.xml
Update Connection Pool File egpl_ds_connpool_map.xml
Extract a Template From the EAR
Remove a Template From the EAR
Add or Update a Template in the EAR
Add Custom JARS Required for Customization
Add New Custom Classes Required for Customization
Add New Java Data Adapter Classes Required for Customization
Add New Query and Schema Files Required for Customization

Add New Custom Rules to be used in WorkFlows

Changes on the Service Server

**To add a new custom rule to egpl_custom.jar:**

1. Copy the custom rules classes into a temporary folder on the machine.
2. Create a backup of `Cisco_Home/eservice/lib/custom/egpl_custom.jar` on the Services Server.
3. Start the PackIt utility.
4. From the Task Group menu, select *WorkFlow tasks*.
5. From the Task to perform menu, select *Add custom rules for WorkFlow on Services Server*.
6. Select the `egpl_custom.jar` that needs to be updated.
7. Select the source folder where the custom rule classes are located.
8. Click **Execute** to run PackIt.
9. This adds the new custom rules (with same package structure as in source folder) into the `egpl_custom.jar`.
10. An entry is be made for all custom rules in the `egpl_custom.jar/METAINF/services/com.egain.platform.module.routing.CustomRule` file.
Changes to the EAR

As a best practice, maintain identical jars on the Services Server and in the EAR.

To add a new custom rule to the EAR:
1. Copy the folder with the custom rule classes to a temporary location.
2. Create a backup of the EAR that is in the installation folder on the File Server.
3. Start the PackIt utility.
4. From the Task Group menu, select WorkFlow tasks.
5. From the Task to perform menu, select Add custom rules for WorkFlow in EAR.
6. Select the eService.ear that needs to be updated.
7. Select the source folder where the custom rule classes are located.
8. Click Execute to start PackIt.
9. This adds the new custom rules (with the same package structure as in the source folder) into egpl_custom.jar inside the EAR.
10. An entry is made for all the custom rules in eService.ear/lib/custom/egpl_custom.jar/META-INF/services/com.egain.platform.module.routing.CustomRule file.

Add New Custom Conditions to be used in WorkFlows

Changes on the Service Server

To add a new custom condition to egpl_custom.jar:
1. Copy the custom conditions classes into a temporary folder on the machine.
2. Create a backup of Cisco_Home/eservice/lib/custom/egpl_custom.jar on the Services Server.
3. Start the PackIt utility.
4. From the Task Group menu, select WorkFlow tasks.
5. From the Task to perform menu, select Add custom conditions for WorkFlow on Services Server.
6. Select the egpl_custom.jar that needs to be updated.
7. Select the source folder where the custom condition classes are located.
8. Click Execute to run PackIt.
9. This adds the new custom conditions (with the same package structure as in the source folder) into egpl_custom.jar.
10. An entry is made for all the custom conditions in egpl_custom.jar/META-INF/services/com.egain.platform.module.routing.CustomCondition file.
Changes to the EAR

As a best practice, maintain identical jars on the Services Server and in the EAR.

To add a new custom condition to the EAR:
1. Copy the folder with the custom condition classes to a temporary location on the machine.
2. Create a backup of the EAR that is in the installation folder on the File Server.
3. Start the PackIt utility.
4. From the Task Group menu, select WorkFlow tasks.
5. From the Task to perform menu, select Add custom conditions for WorkFlow in EAR.
6. Select eServices.ear that needs to be updated.
7. Select the source folder where the custom condition classes are located.
8. Click Execute to run PackIt.
9. This adds the new custom conditions (with the same package structure as in the source folder) into egpl_custom.jar inside EAR.
10. An entry is made for all the custom conditions in eService.ear/lib/custom/egpl_custom.jar/META-INF/services/com.egain.platform.module.routing.CustomCondition file.

Add New Connection Pools for SQL JDBC Data Adapters

Changes to the EAR

To add a new connection pool:
1. Create a backup of the EAR that is in the installation folder on the File Server.
2. Start the PackIt utility.
3. From the Task Group menu, select Connection Pool tasks.
4. From the Task to perform menu, select Add connection pool in EAR.
5. Select eServices.ear that needs to be updated.
6. Provide entries in the Database Connection Pool Section for each field. Please note only required fields are enabled on GUI so its important to provide correct value for the fields.
7. Click Execute to run PackIt.
8. This will add the new connection pool in egpl_ds_connpool_map.xml file in configurations.zip inside EAR.

Changes on the Service Server

To add a new connection pool to configurations.zip:
1. Create a backup of Cisco_Home/eservice/lib/configurations.zip on Services Server.
2. Start the PackIt utility.
3. From the Task Group menu, select **Connection Pool tasks**.

4. From the Task to perform menu, select **Add connection pool on Services Server**.

5. Select the `configurations.zip` in the `lib` folder on the services server that needs to be updated.

6. Provide entries in Database Connection Pool Section for each field. Note that only required fields are enabled in the user interface, so it's important to provide the correct values for the fields.

7. Click the **Execute** button to run PackIt.

8. This adds the new connection pool in `egpl_ds_connpool_map.xml` file in `configurations.zip`.

---

### Update Connection Pools for SQL JDBC Data Adapters

#### Changes to the EAR

**To update the connection pool:**

1. Create a backup of the EAR that is in the installation folder on the File Server.

2. Start the PackIt utility.

3. From the Task Group menu, select **Connection Pool tasks**.

4. From the Task to perform menu, select **Update connection pool in EAR**.

5. Select the `eServices.ear` that needs to be updated.

6. Provide entries in the Database Connection Pool Section for each field. Note that only required fields are enabled in the user interface, so it's important to provide the correct values for the fields.

7. Click the **Execute** button to run PackIt.

8. This updates the connection pool in `egpl_ds_connpool_map.xml` file in `configurations.zip` inside the EAR. If the pool does not exist in the file, it does not make any change.

#### Changes on the Service Server

**To update the connection pool in configurations.zip:**

1. Create a backup of `Cisco_Home/eservice/lib/configurations.zip`.

2. Start the PackIt utility.

3. From the Task Group menu, select **Connection Pool tasks**.

4. From the Task to perform menu, select **Update connection pool on Services Server**.

5. Select the `configurations.zip` in the `lib` folder on the services server that needs to be updated.

6. Provide entries in the Database Connection Pool Section for each field. Note that only required fields are enabled in the user interface, so it's important to provide the correct values for the fields.

7. Click the **Execute** button to run PackIt.

8. This updates the connection pool in `egpl_ds_connpool_map.xml` file in `configurations.zip`. If the pool does not exist in the file, it does not make any change.
Remove a Redundant Connection Pool

**Changes to the EAR**

**To remove a connection pool:**

1. Create a backup of the EAR that is in the installation folder on the File Server.
2. Start the PackIt utility.
3. From the Task Group menu, select *Connection Pool tasks*.
4. From the Task to perform menu, select *Remove connection pool in EAR*.
5. Select the `eservices.ear` that needs to be updated.
6. Provide entries in Database Connection Pool Section for the name of pool that needs to be removed.
7. Click the *Execute* button to run PackIt.
8. This removes the connection pool in `egpl_ds_connpool_map.xml` file in `configurations.zip` inside the EAR. If the pool does not exist in the file, it does not make any change.

**Changes on the Service Server**

**To remove a connection pool from configurations.zip:**

1. Create a backup of `Cisco_Home/eservice/lib/configurations.zip`.
2. Start the PackIt utility.
3. From the Task Group menu, select *Connection Pool tasks*.
4. From the Task to perform menu, select *Remove connection pool on Services Server*.
5. Select the `configurations.zip` in the `lib` folder on the services server that needs to be updated.
6. Provide entries in Database Connection Pool Section for the name of the pool that needs to be removed.
7. Click the *Execute* button to run PackIt.
8. This removes the connection pool in `egpl_ds_connpool_map.xml` file in `configurations.zip`. If the pool does not exist in the file, it does not make any change.

**Extract Connection Pool File egpl_ds_connpool_map.xml**

**From the EAR**

**To extract the `egpl_ds_connpool_map.xml` file:**

1. Create a backup of the EAR that is in the installation folder on the File Server.
2. Start the PackIt utility.
3. From the Task Group menu, select *Connection Pool tasks*.
4. From the Task to perform menu, select **Extract connection pool file from EAR**.
5. Select the `eservices.ear` from where you need to extract the connection pool file.
6. Provide the location of the destination folder to which you wish to extract the file.
7. Click the **Execute** button to run PackIt.
8. This extracts the `egpl_ds_connpool_map.xml` file from `configuration.zip` folder inside the EAR.

**From the Services Server**

**To extract the connection pool file from configurations.zip:**

1. Create a backup of `Cisco_Home/eservice/lib/configurations.zip`.
2. Start the PackIt utility.
3. From the Task Group menu, select **Connection Pool tasks**.
4. From the Task to perform menu, select **Extract Connection Pool from ZIP on Services Server**.
5. Select the `configurations.zip` in the `lib` folder on the services server from which to extract `egpl_ds_connpool_map.xml` file.
6. Provide the location of the destination folder to which you wish to extract the file.
7. Click the **Execute** button to run PackIt.
8. This extracts the connection pool in `egpl_ds_connpool_map.xml` file in `configurations.zip`.

**Update Connection Pool File egpl_ds_connpool_map.xml**

**Changes to the EAR**

**To update the egpl_ds_connpool_map.xml file:**

1. Create a backup of the EAR that is in the installation folder on the File Server.
2. Start the PackIt utility.
3. From the Task Group menu, select **Connection Pool tasks**.
4. From the Task to perform menu, select **Update connection pool in EAR**.
5. Select the `eservices.ear` that needs to be updated.
6. Select the source folder where the updated `dataaccess/egpl_ds_connpool_map.xml` file is located.
7. Click the **Execute** button to run PackIt.
8. This updates the `egpl_ds_connpool_map.xml` file in `configuration.zip` inside the EAR.
Changes on the Services Server

To update the connection pool file in configurations.zip:
1. Create a backup of Cisco_Home/eservice/lib/configurations.zip.
2. Start the PackIt utility.
3. From the Task Group menu, select Connection Pool tasks.
4. From the Task to perform menu, select Update Connection Pool in ZIP on Services Server.
5. Select the configurations.zip in the lib folder on the services server that needs to be updated.
6. Select the source folder where the updated dataaccess/egpl_ds_connnpool_map.xml file is located.
7. Click the Execute button to run PackIt.
8. This updates the egpl_ds_connnpool_map.xml file in configurations.zip.

Extract a Template From the EAR

All old chat templates upgraded from previous versions of Unified EIM and WIM 9.0(1) are bundled in the chattemplates.WAR WAR file inside the EAR.

To extract a template from the EAR:
1. Create a backup of the EAR that is in the installation folder on the File Server.
2. Start the PackIt utility.
3. From the Task Group menu, select Template tasks.
4. From the Task to perform menu, select one of the following items.
   o To extract Chat templates, select Extract Chat templates from EAR
5. Select the eServices.ear from where you need to extract the selected templates.
6. Provide the name of the template that needs to be extracted.
7. Provide the location of the destination folder to which you wish to extract the templates.
8. Click the Execute button to run PackIt.
9. This extracts the selected template from inside EAR. If there is no template in the EAR with that name, nothing is extracted.

Remove a Template From the EAR

All old chat templates upgraded from previous versions of Unified EIM and WIM 9.0(1) are bundled in the chattemplates.WAR WAR file inside the EAR.

To remove a template from the EAR:
1. Create a backup of the EAR that is in the installation folder on the File Server.
2. Start the PackIt utility.
3. From the Task Group menu, select Template tasks.

4. From the Task to perform menu, select one of the following items.
   - To remove Chat templates, select Remove Chat templates from EAR

5. Select the eServices.ear from where you need to remove the selected templates.

6. Provide the name of the template that needs to be removed.

7. Click the Execute button to run PackIt.

8. This removes the selected template from inside the EAR. If there is no template in the EAR with that name, nothing is removed.

**Add or Update a Template in the EAR**

All old chat templates upgraded from previous versions of Unified EIM and WIM 9.0(1) are bundled in the chattemplates.WAR WAR file inside the EAR.

**To add or update a template in the EAR:**

1. Create a backup of the EAR that is in the installation folder on the File Server.
2. Start the PackIt utility.
3. From the Task Group menu, select Template tasks.
4. From the Task to perform menu, select Add or Update templates in EAR.
5. Select the eServices.ear from where you need to add or update templates.
6. Select the Template Type based on the product for which templates are being added or updated.
7. Select the name of the template that needs to be added or updated.
8. Select the source folder from where the new or updated templates are to be picked up.
9. Click the Execute button to run PackIt.
10. This adds the selected template to the correct WAR file inside the EAR.

**Add Custom JARS Required for Customization**

**Changes to the EAR**

Any third-party JAR added for customization needs to go in lib/custom folder inside EAR. An entry for all those JARs are also made in MANIFEST.MF file of egpl_custom.jar so that they are added in classpath without needing to change any .bat files.

**To add custom JARS to the EAR:**

1. Create a backup of the EAR that is in the installation folder on the File Server.
2. Start the PackIt utility.
3. From the Task Group menu, select Miscellaneous tasks.
4. From the Task to perform menu, select **Add custom jars in EAR**.

5. Select the location of the EAR that needs to be updated.

6. Select the source folder where the new JARs are located.

7. Click the **Execute** button to run PackIt.

8. This adds the new jars in lib/custom folder inside the EAR. It also makes an entry for all the JARs with the right path in MANIFEST.MF file of egpl_custom.jar file.

**Changes on the Service Server**

Any third-party JAR added for customization needs to go in lib/custom folder inside EAR. An entry for all those JARs are also made in MANIFEST.MF file of egpl_custom.jar so that they are added in classpath without needing to change any .bat files.

**To add custom JARS to egpl_custom.jar:**

1. Create a backup of the `Cisco_Home/eservice/lib/custom/egpl_custom.jar`.

2. Start the PackIt utility.

3. From the Task Group menu, select **Miscellaneous tasks**.

4. From the Task to perform menu, select **Add custom jars on Services Server**.

5. Select the `egpl_custom.jar` file that needs to be updated.

6. Select the source folder where the new JARs are located.

7. Click the **Execute** button to run PackIt.

8. This adds the new jars into the `Cisco_Home/eservice/lib/custom` folder where `egpl_custom.jar` is located. It also makes an entry for all the JARs with the right path in MANIFEST.MF file of `egpl_custom.jar` file.

**Add New Custom Classes Required for Customization**

**Changes to the EAR**

Any new custom classes need to go in the `/lib/custom/egpl_custom.jar` inside the EAR.

**To add custom classes to the EAR:**

1. Create a backup of the EAR that is in the installation folder on the File Server.

2. Start the PackIt utility.

3. From the Task Group menu, select **Miscellaneous tasks**.

4. From the Task to perform menu, select **Bundle custom classes inside EAR**.

5. Select the location of the EAR that needs to be updated.

6. Select the source folder where the new classes are located.
7. Click the **Execute** button to run PackIt.
8. This adds the new classes in `lib/custom/egpl_custom.jar` inside the EAR.

**Changes on the Service Server**

Any new custom classes need to go in the `/lib/custom/egpl_custom.jar` on Services Server.

**To add custom classes to egpl_custom.jar:**
1. Create a backup of `egpl_custom.jar` on the Services Server.
2. Start the PackIt utility.
3. From the Task Group menu, select **Miscellaneous tasks**.
4. From the Task to perform menu, select **Bundle custom classes on Services Server**.
5. Select the location of the `egpl_custom.jar` that needs to be updated.
6. Select the source folder where the new classes are located.
7. Click the **Execute** button to run PackIt.
8. This adds the new classes in `lib/custom/egpl_custom.jar` on the Services Server.

**Add New Java Data Adapter Classes Required for Customization**

**Changes to the EAR**

Any new custom classes need to go in the `/lib/custom/egpl_custom.jar` inside the EAR.

**To add Java data adapter classes to the EAR:**
1. Create a backup of the EAR that is in the installation folder on the File Server.
2. Start the PackIt utility.
3. From the Task Group menu, select **Miscellaneous tasks**.
4. From the Task to perform menu, select **Bundle custom classes inside EAR**.
5. Select the location of the EAR that needs to be updated.
6. Select the source folder where the new classes are located.
7. Click the **Execute** button to run PackIt.
8. This adds the new Java Data Adapter classes in `lib/custom/egpl_custom.jar` inside the EAR.
Changes on the Service Server

Any new custom classes need to go in the /lib/custom/egpl_custom.jar on Services Server.

To add Java data adapter classes to egpl_custom.jar:
1. Create a backup of egpl_custom.jar on the Services Server.
2. Start the PackIt utility.
3. From the Task Group menu, select Miscellaneous tasks.
4. From the Task to perform menu, select Bundle custom classes on Services Server.
5. Select the location of the egpl_custom.jar that needs to be updated.
6. Select the source folder where the new classes are located.
7. Click the Execute button to run PackIt.
8. This adds the new Java Data Adapter classes in lib/custom/egpl_custom.jar on the Services Server.

Add New Query and Schema Files Required for Customization

Changes to the EAR

Any new custom classes need to go in the configurations_custom.zip inside the EAR.

To add new query and schema files to the EAR:
1. Create a backup of the EAR that is in the installation folder on the File Server.
2. Start the PackIt utility.
3. From the Task Group menu, select Miscellaneous tasks.
4. From the Task to perform menu, select Bundle custom schema or query files inside EAR.
5. Select the location of the EAR that needs to be updated.
6. Select the source folder where the new schema or query files are located.
7. Click the Execute button to run PackIt.
8. This adds the new files to configurations_custom.zip inside the EAR.

Changes on the Service Server

Any new custom classes need to go in the configurations_custom.zip on Services Server.

To add new query and schema files to egpl_custom.jar:
1. Create a backup of egpl_custom.jar on the Services Server.
2. Start the PackIt utility.
3. From the Task Group menu, select Miscellaneous tasks.
4. From the Task to perform menu, select **Bundle custom schema or query files on Services Server**.
5. Select the location of the `egpl_custom.jar` that needs to be updated.
6. Select the source folder where the new schema or query files are located.
7. Click the **Execute** button to run PackIt.
8. This adds the new files to `configurations_custom.zip` on the Services Server.