Cisco Unified Web and E-Mail Interaction Manager Troubleshooting Guide
For Unified Contact Center Enterprise

Release 11.0(1)
August 2015

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

Preface ...............................................................................................................................................13
  About This Guide . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14
  Obtaining Documentation and Submitting a Service Request . . . . . . . . . . . . . . . . . . . . . 14
  Documentation Feedback . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14
  Field Alerts and Field Notices . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 15
  Document Conventions. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 15
  Other Learning Resources. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 15
  Online Help . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 15
  Document Set . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 16

Chapter 1: Getting Started...............................................................................................................17
  Pre-Requisites . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .1 8
  Using This Guide . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 18
  Presentation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 18
  Note About Log Files . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 18

Chapter 2: Troubleshooting Tools .................................................................................................20
  List of Activity and Case Statuses . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 21
  List of Processes and Log Files. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 24
  Configuring Cleanup of Logs Folder . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 25
  Tracing Levels for Troubleshooting Issues. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 26
  Cisco Unified EIM & WIM and Unified CCE Integration Messages . . . . . . . . . . . . . . . . 26
    EAAS and MR Communication Messages . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 27
    Communication Session Request and Response Messages. . . . . . . . . . . . . . . . . . . . 27
    Task Routing Messages. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 28
  Listener and CTI Server Communication Messages . . . . . . . . . . . . . . . . . . . . . . . . . . 30
    Communication Session Request and Response Messages. . . . . . . . . . . . . . . . . . . . 30
    Agent Reporting Messages . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 31
    Task Reporting Messages . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 32
    Agent Interruption Messages. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 34
Session Synchronization Messages ................................. 35
UI Debugging Tools ..................................................... 37
F12 Developer Tools .................................................... 37
To enable the F12 developer tools in Internet Explorer: ............... 37
Request Response Data and UI Logging Utility ....................... 38
About the Utility ......................................................... 38
Log Files ................................................................. 38
Logging Utility Options ................................................ 38
Fiddler or HttpWatch .................................................... 40
To Troubleshoot With Fiddler or HttpWatch: ......................... 40
Cisco Unified Web and E-Mail Interaction Manager Debugger .... 41
Java Debugging .......................................................... 42
Enabling the Java Console ............................................. 42
Capturing Logs from the Java Console ............................... 43
Capturing Java Logs From the File System .......................... 43
Server Debugging Tools ............................................... 43
Generating Thread Dumps and Heap Dumps ......................... 43
About Thread Dumps .................................................... 43
About Heap Dumps ...................................................... 44
About the Thread Dump Utility ....................................... 44
Thread Dump Utility Configuration .................................. 44
Creating a Thread Dump ............................................... 44
Viewing Attachments Stored in Database ............................ 45

Chapter 3: General Issues ............................................................................................................... 46

Installation Issues .......................................................... 47
About Installation Logs .................................................... 47
Symptom 1: “Unable to Connect to Database” Error During Installation .... 47
  Cause 1: SQL Server Service Not Running .......................... 47
  Cause 2: TCP/IP Protocol is Disabled ............................... 47
  Cause 3: TCP Port Blocked by Firewall ............................. 48
Symptom 2: “Unable to Create Database” Error During Installation .... 49
  Cause 1: Not Enough Space Available on Database Machine ....... 49
  Cause 2: Correct Permissions Not Assigned to Database Administrator User . 50
Symptom 3: Unable to Start the Unified EIM and WIM Windows Service .... 50
  Cause: Incorrect Domain User Name and Password Information ........ 50
Symptom 4: Unable to Run the Unified EIM and WIM Upgrade Installer .... 51
  Cause 1: Application Server Not Listed in Product Information Window .... 51
  Cause 2: Messaging Server Not Listed in Product Information Window .... 52
  Cause 3: Services Server Not Listed in Product Information Window .... 52
Cause 4: Web Server Not Listed in Product Information Window  
Symptom 5: “Access Denied” Error While Running Upgrade Installer  
Cause 1: Files Under the File Server Installation Folder are Read-Only  
Cause 2: Files Under the File Server Installation Folder are In Use  
Application Start-up Issues  
Symptom: Application Not Starting on All servers  
Cause 1: Required Ports Not Available  
Cause 2: All Unified EIM & WIM Components Not Updated to Same Version  
Cause 3: Low Disk Space  
Cause 4: EAR Deployment Timed Out  
Logging In Issues  
Symptom 1: 404 Error Page Displayed While Logging In  
Cause: Context Root Name in the URL is Incorrect  
Symptom 2: Internal Server Error Page Displayed While Logging In  
Cause: Permissions Not Assigned for egain-plugin Folder  
Symptom 3: Internet Explorer Cannot Display Webpage When Logging In  
Cause: Web Server Not Running  
Login Issues  
Overview  
Symptom 1: “Login Not Successful to One or More MRDs” Error Message  
Cause: MRD Missing From Application Path Member List  
Symptom 2: “Login timed out with Unified CCE” Error Displayed on Login  
Cause 1: Listener Service Process or Instance Not Running  
Cause 2: Media_Login_Resp Message Not Returned Within Timeout Interval  
Symptom 3: “Log Out Now” Error Message Displayed on Login  
Cause 1: Primary Unified CCE AW Database Not Configured Correctly  
Cause 2: Secondary Unified CCE AW Database Not Configured Correctly  
Cause 3: Unified CCE AW Database Connection Pool Limit Exceeded  
Symptom 4: Agents Unable to Login  
Cause 1: Services Required for Successful Login Not Running  
Cause 2: Agent Not Associated With Any MRD  
Logout Issues  
Overview  
Symptom: Activities Routed to Logged Out Agents  
Cause 1: Agent Logout Status Not Updated in Unified CCE  
Cause 2: Synchronization of Agent Login State Fails  
User Interface Issues  
Symptom 1: Blank Consoles Displayed  
Symptom 2: Hourglass Appears When Performing Certain Console Actions
Cause 1: Agent Desktop Not Configured Properly ........................................... 68
Cause 2: Internet Explorer Browser Hangs ......................................................... 68
Cause 3: Other Applications on User Desktop Using High CPU ....................... 68
Cause 4: Other Applications on User Desktop Using High Memory ................. 69
Cause 5: Application Using High CPU and Memory on User Desktop .............. 69
Cause 6: Issues on Server Side ........................................................................... 70
Cause 7: Database Issue .................................................................................... 70
Further Actions .................................................................................................. 71

Chapter 4: Unified CCE Configuration Issues ......................................................... 72

Overview ............................................................................................................ 73

Configuration Issues .......................................................................................... 73
Symptom 1: Listener Instance Stuck in “Connecting” State ................................. 73
  Cause: Incorrect Application Path in Unified CCE for the Peripheral Gateway 73
Symptom 2: MR PIM Stuck on “Attempting to Connect to MR Application…” . . 74
  Cause: MR PIM Port Does Not Match EAAS Instance Port ......................... 74

Chapter 5: Retriever Issues .................................................................................. 77

Overview ............................................................................................................ 78

Email Retrieval Issues ........................................................................................ 78
Symptom 1: Agents Not Receiving Email ............................................................ 78
  Cause 1: Alias Not Added to Retriever Instance .............................................. 78
  Cause 2: Retriever Service Not Running ......................................................... 78
  Cause 3: Alias Not Configured Properly ......................................................... 79
  Cause 4: Certificate Not Installed Properly for SSL Enabled Alias ................. 80
  Cause 5: Non-SSL Account Configured as SSL ............................................ 81
  Cause 6: Retriever Service Hangs ................................................................. 81
Symptom 2: Administrator Gets “Large Email has Been Received” Notification . 82
  Cause: Email Size is Larger Than ‘Maximum Email Size’ Setting .................. 82
Symptom 3: Attachments Missing From Emails ................................................. 82
  Cause: Particular File Extensions are Blocked .............................................. 82
Symptom 4: Emails Retrieved Very Slowly ....................................................... 83
  Cause 1: Database Slowness ......................................................................... 83
  Cause 2: Services Server and POP3 Servers are on Different Networks ........ 83
Symptom 5: Administrator Gets Retriever - Skipping Email Retrieval Notification . 84
  Cause 1: Email is Retrieved but Not Deleted in Previous Cycle .................. 84
  Cause 2: Duplicate Email is Received ........................................................... 85

Email Parsing Issues .......................................................................................... 85
Symptom 1: “Email Reading Failure” Notification Sent to Administrators ........ 85
Chapter 6: Dispatcher Issues

Overview

Setup and Performance Issues
Symptom 1: Dispatcher Service Hangs or Crashes
  Cause: The System has Insufficient Memory
Symptom 2: Unable to Connect to SMTP or ESMTP Server
  Cause 1: SMTP or ESMTP Server Unavailable
  Cause 2: Connections to SMTP or ESMTP Server Exceed Maximum Number
  Cause 3: Connection Times Out
Email Dispatch Issues
Symptom 1: Emails Not Dispatched
  Cause 1: Incorrect SMTP or ESMTP Information
  Cause 2: Port 25 Blocked on Services Server
  Cause 3: Services Server IP Address Blocked on SMTP Server
  Cause 4: Emails Considered as Spam by SMTP Server
  Cause 5: Attachments Considered as Malicious by SMTP Server
  Cause 6: Email Size Exceeds Maximum Allowed Size
  Cause 7: “Read” Permission Not Granted on the Storage Directory
  Cause 8: Relaying Not Allowed for To Addresses of Emails
  Cause 9: Certificate Not Installed Properly for SSL Enabled Alias
  Cause 10: Non-SSL Account Configured as SSL
Symptom 2: Agent Receives Attachment Size Error Message
  Cause: Email Attachment’s Size Larger Than Outgoing Email Size Limit
Symptom 3: Agent Receives Email Content Size Error Message
  Cause: Email Body Size Larger Than Outgoing Email Size Limit
Symptom 4: Agent Receives Email Size Error Message
  Cause: Email Size Larger Than Outgoing Email Size Limit

Chapter 7: Integration Services Issues

Overview

Listener Service Issues
Symptom 1: “Listener Instance Cannot be Started” Error Displayed
  Cause 1: Primary Unified CCE AW Database Not Configured Correctly
  Cause 2: Secondary Unified CCE AW Database Not Configured Correctly
Symptom 2: Listener Instance Stuck in Connecting State
Chapter 8: Email and Workflow Issues

Overview ................................. 101

Activity Routing Issues ............................... 101

A Note About Routing ............................... 101

Symptom 1: Activities Routed to Exception Queue ......... 101
  Cause 1: Inbound Workflow Does Not Exist ......... 101
  Cause 2: End Node in Inbound Workflow is an Inactive Workflow .... 102
  Cause 3: Transfer Node in Inbound Workflow is an Inactive Workflow .... 102
  Cause 4: Inactive Queue in Inbound Workflow ......... 102
  Cause 5: Emails are Bounced Back ............. 103
  Cause 6: Database Queries for Workflow Taking Long Time .... 103
  Cause 7: NEW_TASK_FAILURES Message With Different Reason Codes .... 103

Further Analysis ............................... 105

Symptom 2: Activities Not Routed to Agents ......... 106
  Cause 1: Primary Unified CCE AW Database Not Configured Correctly .... 106
  Cause 2: Secondary Unified CCE AW Database Not Configured Correctly .... 106
  Cause 3: Unified CCE AW Database Connection Pool Limit Exceeded .... 106
  Cause 4: ECC Variables Not Configured Properly .... 106
  Cause 5: Media Router of Unified CCE Unable to Connect to EAAS Instance .... 107
  Cause 6: MRD Task Limit Met ......... 108
  Cause 7: Unified CCE Script Selector Not Configured Properly .... 108
  Cause 8: Unified CCE Script Not Configured Properly .... 108
  Cause 9: Concurrent Task Limit of Agent Met ......... 109
  Cause 10: Media Class Not Configured Properly .... 109

Symptom 3: NIPTA Routing is Not Working ......... 110
  Cause 1: NIPTA Routing Disabled ......... 110
  Cause 2: NIPTA Agents Not Mapped to User Groups in Unified EIM & WIM .... 111
  Cause 3: Unified CCE Script Labels Not Configured Correctly .... 111

Symptom 4: Activities Routed to Incorrect Agents .... 111
  Cause: Media Router Responds to NEW_TASK Without An Agent ID .... 112

Symptom 5: Agent Unable to Create Outbound Emails .... 112
  Cause: Agent Not Configured For Outbound MRD .... 112

Symptom 6: Agent Sees Error About Completing Non-Interruptible Activities .... 113
  Cause: Outbound MRD Interrupted for Agent ......... 113
Symptom 7: Agent Sees Maximum Number of Outbound Activities Error
Caused: Agent Concurrent Task Limit Met

Symptom 8: Email Activities Assigned After Long Delay
Caused: OFFER_TASK_IND Message Sent After Delay

Chapter 9: Chat Issues

Chat Assignment Issues

Symptom 1: Delay in Chat Assignment
Caused 1: All Agents Have Reached Maximum Load
Caused 2: Activities Pushed Back to Queue
Further Actions

Symptom 2: Chats Not Assigned to Agents
Caused 1: Primary Unified CCE AW Database Not Configured Correctly
Caused 2: Secondary Unified CCE AW Database Not Configured Correctly
Caused 3: Unified CCE AW Database Connection Pool Limit Exceeded
Caused 4: Queues Not Configured to Route Chats
Caused 5: Queue Not Mapped to Correct MRD
Caused 6: Agents Unavailable to Receive Chats
Caused 7: All Agents Have Reached Maximum Load
Caused 8: Script Error Occurs in the Agent Console
Caused 9: Problems With Agent Assignment Service
Caused 10: Problems With JMS Messaging
Caused 11: Problems With Event Messaging
Further actions

Chat Session Issues

Symptom 1: Error Message Displayed When Chat Agent Logs In
Caused 1: Entry Point Not Active
Caused 2: Agents Not Available
Caused 3: Agent Assignment Service Not Started
Caused 4: EAAS Service Not Started
Caused 5: Chat Queueing Disabled For Integrated Chat Agents
Further actions
Caused 6: EAAS Not Connected to Media Router

Symptom 3: Customers see “System Cannot Assign an Agent to the Request”
Caused: No Chat Agents Logged in to Unified EIM and WIM

Symptom 4: “Lines are Busy” Message Displayed to Chat Customers
Caused 1: Chat Activity Abandoned by the Watchdog Thread
Caused 2: All Integrated Chat Agents Have Reached Concurrent Task Limit

Symptom 5: Wait Template Not Displayed to Chat Customers
Caused: Incorrect Tags Configured in DRASR Configuration File
Symptom 6: Customer Chat Status Changes to “Slow But Still Connected” . . . . . . 133
Symptom 7: Chat Messages Not Delivered to Agents or Customers . . . . . . . 134
  Cause 1. Connection Issues to Application Server . . . 134
  Cause 2. Problems With Event Messaging . . . . . . 134

Chapter 10: Offers Issues ..................................................................................................................135
Offers Display Issues ............................................................................................................................136
Symptom 1: Offers Not Displayed on Web Pages ............................................................................. 136
  Cause 1: Offer Enablement Code Not Added to Web Pages . . . . . . . . . 136
  Cause 2: Incorrect Page URL Configured . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 136
  Cause 3: Offers Not Activated . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 136
  Cause 4: Eligibility Conditions Not Met . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 137
  Cause 5: Chat Offers Requirements Not Met . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 137
  Cause 6: Offer is Not Configured Relative to the Correct Object . . . . . . . . . . . . . . . . . . . . 137
  Cause 7: Offers Displayed on Specific Browsers Only . . . . . . . . . . . . . . . . . . . . . . . . . . 137
Symptom 2: All Offers Configured for a Web Page Not Displayed . . . . . . . . . . . . . . . . . . . 139
  Cause: Web Page Configured to Display Only One offer 139

Chapter 11: Knowledge Base Issues .................................................................................................140
Multiple Language Knowledge Base Issues .................................................................................. 141
Symptom 1: Import Process of Language Files Fails ..................................................................... 141
  Cause: XML Format Changed in Translations Files . . . . . . . . . . . . . . . . . . . . . . . . . . . . 141
Symptom 2: Attachments Not Displayed in All Languages ................................................................. 141
  Cause: Attachments Not Added to Articles in All Languages . . . . . . . . . . . . . . . . . . . . . . . . . 141
Symptom 3: Changes Made to KB Objects Not Reflected in All Languages . . . . . . . . . . . . . . 142
  Cause: Updated Content Not Translated in All Languages . . . . . . . . . . . . . . . . . . . . . . . . . 142
Symptom 4: Export and Import Translations Buttons Not Available to Authors ................................ 142
  Cause: Actions Not Assigned to Authors . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 142
Symptom 5: Some Folders Missing From Translation File ............................................................... 142
  Cause: Sub-Folders Not Automatically Selected for Translation . . . . . . . . . . . . . . . . . . . . 142
Approval Process Issues .................................................................................................................... 143
Symptom 1: Unable to Edit or Delete Approval Processes .......................................................... 143
  Cause 1: Configured Approval Process has Pending Articles ................................................... 143
  Cause 2: Approval Process has Multiple Approval Levels ....................................................... 143
Symptom 2: Authors Unable to Approve Articles ......................................................................... 144
  Cause 1: Manage Suggestions Permission Not Assigned on Folders .................................. 144
  Cause 2: Approval Process has Multiple Approval Levels ....................................................... 144
Knowledge Workflow Issues .......................................................................................................... 145
Symptom 1: Knowledge Workflows Option is Disabled for Authors .............................................. 145
Chapter 12: Archive Issues .................................................................147

Overview .........................................................................................148

Archive Jobs Issues ...........................................................................148

Symptom 1: Scheduled Archive Jobs Do Not Run .......................148
  Cause 1: Archive Service Not Running .................................148
  Cause 2: Failed Jobs Exist in Application ...............................148
  Cause 3: Stopped Jobs Exist in Department ..............................149
  Further Analysis .................................................................149

Symptom 2: Archive Jobs Fail ...........................................................150
  Cause 1: Database Users Do Not Have Correct Permissions ....150
  Cause 2: Archive Database Unable to Connect to Active Database .150
  Cause 3: Archive Service Not Restarted After Adding Custom Attributes .151
  Cause 4: Transaction Logs are Full .......................................152
  Cause 5: Archive Database is Full .........................................152
  Further Analysis .................................................................153

Purge Jobs Issues ............................................................................153

Symptom 1: Purge Jobs Do Not Run .................................................153
  Cause 1: Archive Service Not Running .................................153
  Cause 2: Failed Purge Jobs Exist in Application .......................153
  Further Analysis .................................................................154

Chapter 13: Reports Issues ...............................................................155

Overview ........................................................................................156

Setup and Performance Issues .........................................................156

Symptom 1: Unable to Run Reports .................................................156
  Cause: Out of Memory Error Causes Reports Service to Fail ...156
Symptom 2: Data Not Moved from Active Database to Reports Database .157
  Cause: Specific Problems With Copying Reports Data ..........157

Report Run and Schedule Issues ....................................................158

Symptom 1: Reports Notifications Not Sent Out .......................158
  Cause: Invalid SMTP Server Settings .................................158
Symptom 2: “Report Service Not Running” Error While Running Reports.  . . . . 158
  Cause: Report Service Not Running ..................................................... 158
Symptom 3: “No Data Found” Message .................................................... 158
  Cause: Summarization Job Not Completed for Specified Date ............... 158
Symptom 4: Error While Viewing Report Results ..................................... 159

Report Results Issues ........................................................................... 160
Symptom: Mismatch in Reports Data ..................................................... 160

Chapter 14: Database Issues ..................................................................161

Overview ............................................................................................... 162
Database Slowness Issues ................................................................. 162
  Symptom: Application Slows Down .................................................. 162
    Cause 1: Inadequate Disk Space ...................................................... 162
    Cause 2: Antivirus Running on Database Server ............................ 162
    Cause 3: Other Applications on the Database Machine Using Disk Space . 163
    Cause 4: Transaction Logs are Full ............................................... 163
    Cause 5: Database Queries Taking Long Time to Run ............... 163
Preface

- About This Guide
- Obtaining Documentation and Submitting a Service Request
- Documentation Feedback
- Field Alerts and Field Notices
- Document Conventions
- Other Learning Resources
Welcome to Cisco® Unified EIM & WIM™, multichannel interaction software used by businesses all over the world to build and sustain customer relationships. A unified suite of the industry’s best applications for web and email interaction management, it is the backbone of many innovative contact center and customer service helpdesk organizations.

Cisco Unified EIM & WIM 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 Troubleshooting Guide* describes recommended actions for the most common issues related to Cisco Unified EIM & WIM.

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

After going through the information provided in this guide, if your problem is still not resolved, collect all the data and results mentioned for your problem, and escalate to Cisco CCBU DE from Cisco TAC. It is very important that you collect all the relevant log files, screenshots, reproductions steps, if possible, and provide those while escalating the issue.

## Obtaining Documentation and Submitting a Service Request


Subscribe to *What’s New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

## Documentation Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.
Field Alerts and Field Notices

Cisco products may be modified or key processes may be determined to be important. These are announced through use of the Cisco Field Alerts and Cisco Field Notices. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

Log into www.cisco.com and then access the tool at http://www.cisco.com/cisco/support/notifications.html

Document Conventions

This guide uses the following typographical conventions.

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

Other Learning Resources

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

Online Help

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

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

- The Cisco Unified Web and E-Mail Interaction Manager documentation is available in the Documents folder on the product CD. The latest versions of all Cisco documentation can be found online at http://www.cisco.com

- All Unified EIM documentation can be found online at http://www.cisco.com/en/US/products/ps7236/tsd_products_support_series_home.html

- All Unified WIM documentation can be found online at http://www.cisco.com/en/US/products/ps7233/tsd_products_support_series_home.html

- In particular, Release Notes for these products can be found at http://www.cisco.com/en/US/products/ps7236/prod_release_notes_list.html

- For general access to Cisco Voice and Unified Communications documentation, go to http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

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 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 Knowledge Base 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 Adapters
- 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
Getting Started

- Pre-Requisites
- Using This Guide
This chapter describes some important pre-requisites and guidelines on using this guide.

Pre-Requisites

Before you start using this guide, make sure that you have:

- Completed the Cisco Unified EIM and WIM training.
- Familiarized yourself with the documents listed in the Document Set section on page 17.

Important: You must meet these requirements before proceeding through the rest of the guide.

Using This Guide

Please be aware that users proceeding through the steps listed in this guide do so at their own risk. Debugging issues in Cisco Unified EIM & WIM may involve changing partition and system level settings, as well as server configurations. Troubleshooting issues improperly may lead to problems with the application itself, including such situations as: inability to open the application, performance degradation, and loss of data. We strongly suggest backing up your data before making any changes that may have an impact on the data in the system.

Presentation

The information in the troubleshooting sections is presented in the following format:

- **Symptom:** First, the symptom of the problem is described. Examples are “Emails are not getting assigned to agents”, “Service unavailable message is displayed to chat customers”, etc.

- **Causes:** Next, the various factors that can cause the problem are described. Some examples are: emails may not be assigned to agents because an alias has not been added to the Retriever service instance, or the “Service unavailable” message is displayed to chat customers because an entry point is not active, etc.

- **Recommended actions:** Finally, for each cause is a list of actions that can be taken to understand and solve the problem. Recommended actions include making sure that components and objects in the system are configured properly, collecting and analyzing log files, etc.

If the problem is still not resolved after going through the Causes and Recommended actions, collect all the data and results mentioned for the issue and escalate the problem to Cisco TAC. It is very important that you collect all the relevant log files, screenshots, and reproductions steps, if possible, and provide those to Cisco TAC when escalating the issue.

Note About Log Files

The reference names of log files, signified by Variable text, indicate the location the log file may be found.
For example, the log file with the name: `eg_log_Services_Server_Name_rules-process.log` can be found on the services server. Similarly, the log file with the name: `eg_log_Application_Server_Name_ApplicationServer.log` can be found under the application server.

**Important:** Do not run any queries on the databases which will alter the information in the database. If you run into such conditions, please do not proceed and contact Cisco TAC for assistance.
Troubleshooting Tools

- List of Activity and Case Statuses
- List of Processes and Log Files
- Configuring Cleanup of Logs Folder
- Tracing Levels for Troubleshooting Issues
- Cisco Unified EIM & WIM and Unified CCE Integration Messages
- UI Debugging Tools
- Server Debugging Tools
- Viewing Attachments Stored in Database
This chapter describes common tools available for troubleshooting. Configuration procedures for these tools, if any, are also described here.

**List of Activity and Case Statuses**

Information about activity and case status, stored in the `egpl_casemgmt_activity` and `egpl_casemgmt_case` tables, is useful for troubleshooting problems with activity routing. This section lists the values for activity status, activity substatus, activity type, activity subtype, activity mode, and case status.

**Activity Status and Substatus**

Activity status names are shown in bold type.

<table>
<thead>
<tr>
<th>Value</th>
<th>Activity status</th>
<th>Activity substatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>1900</td>
<td></td>
<td>In progress</td>
</tr>
<tr>
<td>3000</td>
<td>Workflow</td>
<td></td>
</tr>
<tr>
<td>3100</td>
<td></td>
<td>Ready for inbound workflow</td>
</tr>
<tr>
<td>3200</td>
<td></td>
<td>Ready for outbound workflow</td>
</tr>
<tr>
<td>3300</td>
<td></td>
<td>Ready for general workflow</td>
</tr>
<tr>
<td>3400</td>
<td></td>
<td>Ready for transfer workflow</td>
</tr>
<tr>
<td>3800</td>
<td></td>
<td>Error</td>
</tr>
<tr>
<td>3900</td>
<td></td>
<td>Progress</td>
</tr>
<tr>
<td>4000</td>
<td>Assignment</td>
<td></td>
</tr>
<tr>
<td>4100</td>
<td></td>
<td>Ready for internal assignment</td>
</tr>
<tr>
<td>4105</td>
<td></td>
<td>Ready for Unified CCE routing</td>
</tr>
<tr>
<td>4106</td>
<td></td>
<td>Ready for NIPTA assignment</td>
</tr>
<tr>
<td>4107</td>
<td></td>
<td>Listener picks niPTA agent</td>
</tr>
<tr>
<td>4200</td>
<td></td>
<td>Ready for external assignment</td>
</tr>
<tr>
<td>5000</td>
<td>Assigned</td>
<td></td>
</tr>
<tr>
<td>5100</td>
<td></td>
<td>New</td>
</tr>
<tr>
<td>5200</td>
<td></td>
<td>Pending</td>
</tr>
<tr>
<td>5300</td>
<td></td>
<td>Wrap up</td>
</tr>
<tr>
<td>5900</td>
<td></td>
<td>In progress</td>
</tr>
<tr>
<td>7000</td>
<td>Pre Completion</td>
<td></td>
</tr>
</tbody>
</table>
List of activity statuses and substatuses

**Activity Types and Subtypes**

Activity type names are shown in bold type.

<table>
<thead>
<tr>
<th>Value</th>
<th>Activity type</th>
<th>Activity status</th>
</tr>
</thead>
<tbody>
<tr>
<td>7100</td>
<td>Email</td>
<td>Ready for email dispatch</td>
</tr>
<tr>
<td>7300</td>
<td></td>
<td>Email dispatch in progress</td>
</tr>
<tr>
<td>9000</td>
<td></td>
<td>Completed</td>
</tr>
<tr>
<td>9100</td>
<td></td>
<td>Done</td>
</tr>
<tr>
<td>9200</td>
<td></td>
<td>Abandoned</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value</th>
<th>Activity type</th>
<th>Activity subtype</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Email</td>
<td>General</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Web form</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Secure</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Permanent undeliverable</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Temporary undeliverable</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Reply</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>Forward</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>Compose</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>Auto reply</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>Auto acknowledge</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>Group reply</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>Redirect</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>Undispatch</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>Supervisory accept</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>Supervisory reject</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>Supervisory reattempt</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>Chat Transcript</td>
</tr>
<tr>
<td>8001</td>
<td></td>
<td>General</td>
</tr>
<tr>
<td>2000</td>
<td>Chat</td>
<td></td>
</tr>
<tr>
<td>2001</td>
<td></td>
<td>Text Chat</td>
</tr>
<tr>
<td>Value</td>
<td>Activity type</td>
<td>Activity subtype</td>
</tr>
<tr>
<td>--------</td>
<td>---------------</td>
<td>------------------</td>
</tr>
<tr>
<td>12002</td>
<td></td>
<td>Callback</td>
</tr>
<tr>
<td>12003</td>
<td></td>
<td>Delayed Callback</td>
</tr>
<tr>
<td>10000</td>
<td>Task</td>
<td></td>
</tr>
<tr>
<td>10001</td>
<td></td>
<td>General</td>
</tr>
</tbody>
</table>

List of activity types and subtypes

### Activity Modes

<table>
<thead>
<tr>
<th>Value</th>
<th>Activity mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Inbound</td>
</tr>
<tr>
<td>200</td>
<td>Outbound</td>
</tr>
<tr>
<td>300</td>
<td>None</td>
</tr>
</tbody>
</table>

List of activity modes

### Case Status

<table>
<thead>
<tr>
<th>Value</th>
<th>Case status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Open</td>
</tr>
<tr>
<td>1</td>
<td>Closed</td>
</tr>
<tr>
<td>2</td>
<td>Ready for closure</td>
</tr>
</tbody>
</table>

List of case statuses
# List of Processes and Log Files

This section provides a list of processes available in the system. For each process, we list the name of the log file in which it records information.

<table>
<thead>
<tr>
<th>#</th>
<th>Component</th>
<th>Process name</th>
<th>Log file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Installation program</td>
<td>Server_Name: eGainInstaller</td>
<td>eg_log_Server_Name_eGainInstaller.log</td>
</tr>
<tr>
<td>2.</td>
<td>Updater</td>
<td>Server_Name: upgrade-installer</td>
<td>eg_log_Server_Name Upgrade-installer.log</td>
</tr>
<tr>
<td>3.</td>
<td>Deployment Configuration Utility</td>
<td>Server_Name: eGConfigUtility</td>
<td>eg_log_Server_Name_eGConfigUtility.log</td>
</tr>
<tr>
<td>4.</td>
<td>Distributed Services Manager (DSM)</td>
<td>Services_Server_Name: DSMController</td>
<td>eg_log_Services_Server_Name__DSMController.log</td>
</tr>
<tr>
<td>5.</td>
<td>Distributed Services Manager (DSM)</td>
<td>Services_Server_Name: dsm-registry</td>
<td>eg_log_Services_Server_Name_dsm-registry.log</td>
</tr>
<tr>
<td>6.</td>
<td>Distributed Services Manager (DSM)</td>
<td>Services_Server_Name: HostController</td>
<td>eg_log_Services_Server_Name_HostController.log</td>
</tr>
<tr>
<td>7.</td>
<td>Distributed Services Manager (DSM)</td>
<td>Services_Server_Name: ServerMonitoring</td>
<td>eg_log_Services_Server_Name_ServerMonitoring.log</td>
</tr>
<tr>
<td>8.</td>
<td>Application server</td>
<td>Application_Server_Name: Application Server</td>
<td>eg_log_Application_Server_Name_ApplicationServer.log</td>
</tr>
<tr>
<td>9.</td>
<td>Agent Assignment service process</td>
<td>Services_Server_Name: agent-assignment-process</td>
<td>eg_log_Services_Server_Name_agent-assignment-process.log</td>
</tr>
<tr>
<td>10.</td>
<td>Alarm service process</td>
<td>Services_Server_Name: alarm-rules-process</td>
<td>eg_log_Services_Server_Name_alarm-rules-process.log</td>
</tr>
<tr>
<td>11.</td>
<td>Archive service process</td>
<td>Services_Server_Name: archive_process</td>
<td>eg_log_Services_Server_Name_archive_process.log</td>
</tr>
<tr>
<td>12.</td>
<td>Activity Pushback service process</td>
<td>Services_Server_Name: auto-pushback-process</td>
<td>eg_log_Services_Server_Name_auto-pushback-process.log</td>
</tr>
<tr>
<td>13.</td>
<td>Dispatcher service process</td>
<td>Services_Server_Name: dx-process</td>
<td>eg_log_Services_Server_Name_dx-process.log</td>
</tr>
<tr>
<td>14.</td>
<td>KB Import service process</td>
<td>Services_Server_Name: import-process</td>
<td>eg_log_Services_Server_Name_import-process.log</td>
</tr>
<tr>
<td>15.</td>
<td>Article Rating service process</td>
<td>Services_Server_Name: kb-article-rating-process</td>
<td>eg_log_Services_Server_Name_kb-article-rating-process.log</td>
</tr>
<tr>
<td>16.</td>
<td>Attachment service process</td>
<td>Services_Server_Name: kb-attachment-cs</td>
<td>eg_log_Services_Server_Name_kb-attachment-cs.log</td>
</tr>
<tr>
<td>17.</td>
<td>Report service process</td>
<td>Services_Server_Name: report-process</td>
<td>eg_log_Services_Server_Name_report-process.log</td>
</tr>
<tr>
<td>18.</td>
<td>Workflow Cache service process</td>
<td>Services_Server_Name: rules-cache-process</td>
<td>eg_log_Services_Server_Name_rules-cache-process.log</td>
</tr>
</tbody>
</table>
List of processes and log files

<table>
<thead>
<tr>
<th>#</th>
<th>Component</th>
<th>Process name</th>
<th>Log file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Workflow Engine service process</td>
<td>Services_Server_Name: rules-process</td>
<td>eg_log_Services_Server_Name_rules-process-process.log</td>
</tr>
<tr>
<td>21</td>
<td>Retriever service process</td>
<td>Services_Server_Name: rx-process</td>
<td>eg_log_Services_Server_Name_rx-process-process.log</td>
</tr>
<tr>
<td>22</td>
<td>Scheduler service process</td>
<td>Services_Server_Name: scheduler-process</td>
<td>eg_log_Services_Server_Name_scheduler-process-process.log</td>
</tr>
<tr>
<td>23</td>
<td>Cisco Unified EIM &amp; WIM Integration Wizard</td>
<td>File_Server_Name: ui_config</td>
<td>eg_log_File_Server_Name_ui_config.log</td>
</tr>
<tr>
<td>24</td>
<td>EAAS service process</td>
<td>Services_Server_Name: EAAS-process</td>
<td>eg_log_Services_Server_Name_EAAS-process-process.log</td>
</tr>
<tr>
<td>25</td>
<td>Listener service process</td>
<td>Services_Server_Name: Listener-process</td>
<td>eg_log_Services_Server_Name_Listener-process-process.log</td>
</tr>
<tr>
<td>26</td>
<td>Not in use</td>
<td>knowledge_export</td>
<td>eg_log_knowledge_export.log</td>
</tr>
<tr>
<td>27</td>
<td>Not in use</td>
<td>knowledge_import</td>
<td>eg_log_knowledge_import.log</td>
</tr>
<tr>
<td>28</td>
<td>Not in use</td>
<td>Services_Server_Name: ss-article-rating-process</td>
<td>eg_log_Services_Server_Name_ss-article-rating-process-process.log</td>
</tr>
</tbody>
</table>

**List of processes and log files**

**Configuring Cleanup of Logs Folder**

As you use the product, the Log folders on the servers accumulates log files. To manage the size of your installation folder, it is important to delete old log files periodically.

By default, the system creates log files of up to 5 MB each. Once a log file reaches the maximum size (5 MB), the current file is backed-up as “File_Name.log.<number starting from 1>” (for example, eg_log_V22W2_ApplicationServer.log.1, eg_log_V22W2_ApplicationServer.log.2, etc.) and a new log file is created. If you want a log file’s size to be greater than the default, you can change the value of the Default size in MB setting, where the value of the setting is equivalent to the file’s size in MB.

Backed-up files are automatically deleted after they have reached a certain number. This number can be configured through the Maximum backups of log files setting in the system partition’s Administration Console. After the number of log files reaches the specified value, the system begins deleting the oldest log files in the logs folder to make room for new logs.

Important: It is recommended that you set the value to greater than 50.

To configure the cleanup of logs folder:

- Access the application as a system administrator and from the Administration Console, configure the Logger settings. For details about doing this task, see the Cisco Unified Web and E-mail Interaction Manager Administrator’s Guide to Administration Console.
Tracing Levels for Troubleshooting Issues

- Refer to the following Technical Note for recommended trace levels for troubleshooting and diagnosing Unified CCE issues:
- Refer to the Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to System Console for the trace levels available in Unified EIM and WIM. For the Listener and EAAS process log files, set the log level to info trace level. For all other processes, the trace level should be left at the default level that is the error level. These should be the default levels at which your application should run at all times.

Cisco Unified EIM & WIM and Unified CCE Integration Messages

This section describes the system events and associated messages that are exchanged between various Cisco Unified EIM & WIM and Unified CCE components through the respective interfaces. This section covers system events and message descriptions related to EAAS and MR communication, task routing, and Listener and CTI Server communication (through the ARM interface).
# EAAS and MR Communication Messages

## Communication Session Request and Response Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Message is response to the message or request</th>
<th>Sample message logged in Cisco Unified EIM &amp; WIM Logs</th>
<th>Sample message logged in Unified CCE or CMB Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPEN_REQ</td>
<td>Unified CCE requests EAAS to open and establish a communication session.</td>
<td>—</td>
<td>OPEN_REQ received</td>
<td>OPEN_REQ; Length = 20 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Invoke ID = (2931140) Hex 002cb9c4 HeartbeatInterval = (5000) Hex 00001388</td>
<td>Prior Failure = (0) Hex 00000000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MsgInterfaceRev = (2) Hex 00000002 Hostname: ussuhwvm0040 VersionNumber: 7.0.0.0</td>
<td>Acknowledgement message logged in Unified CCE or CMB Logs</td>
</tr>
<tr>
<td>OPEN_RESP</td>
<td>EAAS responds to the OPEN_REQ with this communication session acknowledgement.</td>
<td>OPEN_REQ</td>
<td>OPEN_RESP send to MR PG sessionId=1 EAASInstanceId=1008</td>
<td>OPEN_RESP; Length = 25 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Invoke ID = (2931140) Hex 002cb9c4 Prior Failure = (0) Hex 00000000 Status = (0) Hex 00000000 Hostname:</td>
<td>Authentication message logged in Unified CCE or CMB Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ussuhwvm0040 VersionNumber: 7.0.0.0</td>
<td>Acknowledgement message logged in Cisco Unified EIM &amp; WIM Logs</td>
</tr>
<tr>
<td>HEARTBEAT_REQ</td>
<td>Unified CCE sends a heartbeat request to EAAS to periodically check the</td>
<td>—</td>
<td>HEARTBEAT_REQ received</td>
<td>HEARTBEAT_REQ; Length = 22 bytes</td>
</tr>
<tr>
<td></td>
<td>communication session.</td>
<td></td>
<td>Invoke ID = (2931140) Hex 002cb9c4</td>
<td>Authentication message logged in Cisco Unified EIM &amp; WIM Logs</td>
</tr>
<tr>
<td>HEARTBEAT_RESP</td>
<td>EAAS responds to the HEARTBEAT_REQ with this positive heartbeat</td>
<td>HEARTBEAT_REQ</td>
<td>HEARTBEAT_RESP</td>
<td>HEARTBEAT_RESP; Length = 22 bytes</td>
</tr>
<tr>
<td></td>
<td>acknowledgement.</td>
<td></td>
<td>Invoke ID = (2931141) Hex 002cb9c5</td>
<td>Authentication message logged in Cisco Unified EIM &amp; WIM Logs</td>
</tr>
<tr>
<td>CLOSE_REQ</td>
<td>Unified CCE requests for gracefully closing the communication session.</td>
<td>—</td>
<td>CLOSE_REQ to MR sessionId=1 EAASInstanceId=1008</td>
<td>CLOSE_REQ; Length = 16 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Invoke ID = (2931142) Hex 002cb9c6 Status: STATUS_ApplicationOffline</td>
<td>Acknowledgement message logged in Cisco Unified EIM &amp; WIM Logs</td>
</tr>
<tr>
<td>CLOSE_RESP</td>
<td>Unified CCE or EAAS responds to the CLOSE_REQ with this communication</td>
<td>CLOSE_REQ</td>
<td>Inside logOutgoingMessage MSG_TYP_CLOSE_RSP</td>
<td>CLOSE_RESP; Length = 16 bytes</td>
</tr>
<tr>
<td></td>
<td>session termination acknowledgement.</td>
<td></td>
<td>Invoke ID = (2931143) Hex 002cb9c7</td>
<td>Authentication message logged in Cisco Unified EIM &amp; WIM Logs</td>
</tr>
</tbody>
</table>
## Task Routing Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Sample message logged in Cisco Unified EIM &amp; WIM Logs</th>
<th>Sample message logged in Unified CCE or CMB Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEW_TASK</td>
<td>EAAS sends this message to ask Unified CCE for instructions on what to do with a new activity.</td>
<td><a href="#">NEW_TASK Message</a> Sent. ActivityId=1091</td>
<td>NEW_TASK, Length = 156 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DialogueID = (6) Hex 00000006</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SendSeqNo = (1) Hex 00000001</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MRDomainID = (5006) Hex 0000138e</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PreviousTask = -1:-1:-1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PreferredAgent = Undefined</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Service = (0) Hex 00000000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CiscoReserved = (0) Hex 00000000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ServiceRequested = (0) for Email/Chat, (1) for Callback (Only for message interface revision 2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ScriptSelector: CV_DN</td>
</tr>
<tr>
<td></td>
<td>NEW_TASK_FAILURE_EVENT</td>
<td><a href="#">NEW_TASK_FAILURE_EVENT</a> received. EAAsInstanceId=1008</td>
<td>NEW_TASK_FAILURE_EVENT T; Length = 12 bytes</td>
</tr>
<tr>
<td></td>
<td>Unified CCE sends this message to tell EAAS that Unified CCE is not able to process the new activity at this time. EAAS can try again with another NEW_TASK message later.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DO_THIS_WITH_TASK</td>
<td>In response to a NEW_TASK request, this message identifies the agent to whom EAAS should assign the activity, or provides a label to EAAS.</td>
<td><a href="#">DO_THIS_WITH_TASK</a> received. EAAsInstanceId=1008</td>
<td>DO_THIS_WITH_TASK; Length = 145 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DialogueID = (5) Hex 00000005</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SendSeqNo = (1) Hex 00000001</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IcmTaskID = 149773:39519200: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SkillGroup = (5196) Hex 0000144c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Service = (5206) Hex 00001456</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Agent = (5168) Hex 00001430</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AgentInfo:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Label: 1058</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Message is response to the message or request</td>
<td>Sample message logged in Cisco Unified EIM &amp; WIM Logs</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>TERMINATE_DIALOGUE_REQ</td>
<td>EAS requests Unified CCE to cancel or terminate a previously established task dialogue.</td>
<td>—</td>
<td>MSG_TYP_TERMINATE_DIALOGUE_REQ</td>
</tr>
<tr>
<td>TERMINATE_DIALOGUE_RESP</td>
<td>Unified CCE sends this message to acknowledge the TERMINATE_DIALOGUE_REQ request from EAAS.</td>
<td>TERMINATE_DIALOGUE_RESP received. EAAInstanceId=1008</td>
<td>—</td>
</tr>
<tr>
<td>REGISTER_VARIABLES_REQ</td>
<td>EAS registers a request for access to the list of Call Variables and Extended Call Context variables.</td>
<td>—</td>
<td>logOutgoingMessage( ) &lt;@&gt; MSG_TYP_REGISTER_VARIABLES_REQ</td>
</tr>
<tr>
<td>REGISTER_VARIABLES_RESP</td>
<td>A response from Unified CCE to EAAS to indicate success or failure of registering the ECC variables.</td>
<td>REGISTER_VARIABLES_REQ</td>
<td>logIncomingMessage( ) &lt;@&gt; MSG_TYP_REGISTER_VARIABLES_RESP</td>
</tr>
<tr>
<td>RUN_APPLICATION_SCRIPT_REQ</td>
<td>Unified CCE instructs EAAS to run an application script known to the application instance.</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>RUN_APPLICATION_SCRIPT_RESULT</td>
<td>EAAS sends the results to Unified CCE after it has executed the application script.</td>
<td>RUN_APPLICATION_SCRIPT_REQ</td>
<td>—</td>
</tr>
<tr>
<td>ROUTING_ENABLED_EVENT</td>
<td>Unified CCE sends this message to EAAS when it is ready to perform media routing services.</td>
<td>—</td>
<td>logIncomingMessage( ) &lt;@&gt; MSG_TYP_ROUTING_ENABLED_EVENT</td>
</tr>
<tr>
<td>ROUTING_DISABLED_EVENT</td>
<td>Unified CCE sends this message to EAAS when it is not ready to perform media routing services.</td>
<td>—</td>
<td>logIncomingMessage( ) &lt;@&gt; MSG_TYP_ROUTING_DISABLED_EVENT</td>
</tr>
</tbody>
</table>
## Listener and CTI Server Communication Messages

### Communication Session Request and Response Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Message is response to the message or request</th>
<th>Sample message logged in Cisco Unified EIM &amp; WIM Logs</th>
<th>Sample message logged in Unified CCE or CMB Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPEN_REQ</td>
<td>Listener requests the CTI Server to establish a communication session.</td>
<td>—</td>
<td>Sending OPEN_REQ</td>
<td>OPEN_REQ (InvokeID:0x1 VersionNumber:9 IdleTimeout:40 PeripheralID:0 ServiceMask:0xc00)</td>
</tr>
<tr>
<td>OPEN_CONF</td>
<td>CTI Server responds to the OPEN_REQ message with this communication session acknowledgement.</td>
<td>OPEN_REQ</td>
<td>OPEN_CONF message received – listenerInstanceId=1008</td>
<td>OPEN_CONF (InvokeID:0x1 ServiceMask:0xc00 MonitorID:0 PGStatus:NORMAL)</td>
</tr>
<tr>
<td>FAILURE_CONF</td>
<td>CTI Server responds to the OPEN_REQ message with negative communication session acknowledgement.</td>
<td>OPEN_REQ</td>
<td>OPEN_REQ Failed. Since session is already terminated so, NOT Closing the Session socket listenerInstanceId, invokeId ,successFailureState</td>
<td>FAILURE_CONF (InvokeID:0x4864 Status:E_CTI_NO_ERROR)</td>
</tr>
<tr>
<td>HEARTBEAT_REQ</td>
<td>Listener sends a heartbeat request to the CTI Server periodically to check the connection of the communication session.</td>
<td>—</td>
<td>Sending HEARTBEAT_REQ</td>
<td>HEARTBEAT_REQ (InvokeID:0x4865 )</td>
</tr>
<tr>
<td>HEARTBEAT_CONF</td>
<td>CTI Server responds to the HEARTBEAT_REQ with this positive heartbeat acknowledgement.</td>
<td>HEARTBEAT_REQ</td>
<td>HEARTBEAT_CONF received and status updated in map for invokeId=402 isAlive=true listenerInstanceId = 2000</td>
<td>HEARTBEAT_RESP (InvokeID:0x4866)</td>
</tr>
<tr>
<td>CLOSE_REQ</td>
<td>Listener requests for gracefully closing the communication session.</td>
<td>—</td>
<td>CLOSE_REQ to MR sessionId=1 EAASInstanceId=2008</td>
<td>CLOSE_REQ (InvokeID:0x4864 Status:E_CTI_NO_ERROR)</td>
</tr>
<tr>
<td>CLOSE_CONF</td>
<td>CTI Server responds to the CLOSE_REQ message with this acknowledgement of termination of the communication session.</td>
<td>CLOSE_REQ</td>
<td>Received CLOSE_CONF</td>
<td>CLOSE_CONF (InvokeID:0x4864)</td>
</tr>
</tbody>
</table>
# Agent Reporting Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Sample message logged in Cisco Unified EIM &amp; WIM Logs</th>
<th>Sample message logged in Unified CCE or CMB Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDIA_LOGIN_REQ</td>
<td>Listener sends agent login request to an MRD.</td>
<td>MEDIA_LOGIN_REQ, AgentId:1005, MRDId:5006</td>
<td>MEDIA_LOGIN_REQ (InvokeId:0x191 MRDId:5006 ARMAgentId:5167 AgentMode:0 IsAvailable:False)</td>
</tr>
<tr>
<td>MEDIA_LOGIN_RESP</td>
<td>CTI Server response to the MEDIA_LOGIN_REQ message.</td>
<td>MEDIA_LOGIN_RESP processing started. listenerInstanceId=1008</td>
<td>MEDIA_LOGIN_RESP (InvokeId:0x191 ARMStatus:E_ARM_STAT_OK)</td>
</tr>
<tr>
<td>MEDIA_LOGOUT_IND</td>
<td>Listener reports agent logout from an MRD.</td>
<td>MEDIA_LOGOUT_IND, AgentId:100, MRDId:5006</td>
<td>MEDIA_LOGOUT_IND (InvokeId:0x1af MRDId:5006 ICMAgentId:5167 Reason:2)</td>
</tr>
<tr>
<td>MAKE_AGENT_ROUTABLE_IND</td>
<td>Listener reports that an agent can be made routable for MRD requests.</td>
<td>Sending MAKE_AGENT_ROUTABLE_IND to ARM for agentId=1005</td>
<td>MAKE_AGENT_ROUTABLE_REQ (InvokeId:0x1af MRDId:5006 ICMAgentId:5167)</td>
</tr>
<tr>
<td>MAKE_AGENT_NOT_ROUTABLE_REQ</td>
<td>Listener reports that an agent should be made not routable for MRD requests.</td>
<td>MAKE_AGENT_NOT_ROUTABLE_REQ to ARM armLoginDataArraySize=ARMAgentData</td>
<td>MAKE_AGENT_NOT_ROUTABLE_RESP (InvokeId:0x1af ArmStatus:E_ARM_STAT_OK)</td>
</tr>
<tr>
<td>MAKE_AGENT_NOT_ROUTABLE_RESP</td>
<td>CTI Server responds to the MAKE_AGENT_NOT_ROUTABLE_REQ message.</td>
<td>MAKE_AGENT_NOT_ROUTABLE_REQ message ARMStatus=E_ARM_STAT_OK listenerInstanceId=2000</td>
<td>MAKE_AGENT_NOT_ROUTABLE_RESP (InvokeId:0x1af ArmStatus:E_ARM_STAT_OK)</td>
</tr>
<tr>
<td>MAKE_AGENT_READY_IND</td>
<td>Listener reports that an agent has been made ready on an MRD.</td>
<td>Sending MAKE_AGENT_READY_IND</td>
<td>MAKE_AGENT_READY_REQ (InvokeId:0x1af MRDId:5006 ICMAgentId:5167 MakeRouteable)</td>
</tr>
<tr>
<td>MAKE_AGENT_NOT_READY_REQ</td>
<td>Listener reports that an agent has been made “not ready” on an MRD.</td>
<td>Sending MAKE_AGENT_NOT_READY_REQ</td>
<td>MAKE_AGENT_NOT_READY_REQ (InvokeId:0x1af MRDId:5006 ICMAgentId:5167 Reason:2)</td>
</tr>
<tr>
<td>MAKE_AGENT_NOT_READY_RESP</td>
<td>CTI Server responds to the MAKE_AGENT_NOT_READY_REQ message.</td>
<td>MAKE_AGENT_NOT_READY_RESP message ARMStatus=E_ARM_STAT_OK listenerInstanceId=2000</td>
<td>MAKE_AGENT_NOT_READY_RESP (InvokeId:0x1af ArmStatus:E_ARM_STAT_OK)</td>
</tr>
</tbody>
</table>
## Task Reporting Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Sample message logged in Cisco Unified EIM &amp; WIM Logs</th>
<th>Sample message logged in Unified CCE or CMB Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFFER_TASK_IND</td>
<td>Listener reports that an agent has been offered a task. The agent is selected by Unified CCE.</td>
<td>OFFER_TASK_IND message Bytes written to Output stream for ActivityId=1006 InstanceId=2000</td>
<td>OFFER_TASK_IND (InvokeID:0x1a3 MRID:5006 ICMAgentID:5167)</td>
</tr>
<tr>
<td>OFFER_TASK_EVENT</td>
<td>CTI Server acknowledges the specified agent has been reserved to handle the specified task.</td>
<td>OFFER_TASK_IND Incoming OFFER_TASK_EVENT pooled in executor for listenerInstanceId = 2000</td>
<td>OFFER_TASK_EVENT: PeripherId=5000 PeripherType=4 MRDomainId=5006</td>
</tr>
<tr>
<td>START_TASK_IND</td>
<td>Listener reports that an agent has started the task. The agent is selected by Unified CCE.</td>
<td>Executing START_TASK_IND for icmAgentId=5241, mrdId=5026, activityId=1006, interruptionState=0</td>
<td>START_TASK_IND (InvokeID:0x5b3e MRID:5026 ICMAgentID:5241 12:06:07 SESSION 3: TaskId:150171/202/1ARMSkillGroupID:5240 ARMServiceID:N/A)</td>
</tr>
<tr>
<td>START_TASK_EVENT</td>
<td>CTI Server acknowledges that the specified agent has started handling the task.</td>
<td>START_TASK_IND Incoming START_TASK_EVENT pooled in executor for listenerInstanceId = 2000</td>
<td>START_TASK_EVENT: PeripherId=5000 PeripherType=4 MRDomainId=5026 12:06:07 Trace: TaskId=150171/202/1ARMSkillGroupID:5240 SkillGroupID=5240 NumNamedVariables:1 NumNamedArrays:0 ScriptSelector:&quot;SS_Email_MRD&quot;</td>
</tr>
<tr>
<td>START_APPLICATION_TASK_REQ</td>
<td>Listener reports that an agent has started the task. The agent is not selected by Unified CCE.</td>
<td>START_APPLICATION_TASK_REQ for icmAgentId=5241, mrdId=5026, activityId=1014, interruptionState=0, isBCTypeMRD=false</td>
<td>START_APPLICATION_TASK_REQ (InvokeID:0x5bad MRID:5026 ICMAgentID:5241 12:22:48 SESSION 3: PreviousICMTaskId:150171/203/1ARMSkillGroupID:5240 ARMServiceID:N/A NumNamedVariables:1 NumNamedArrays:0 ScriptSelector:&quot;SS_Email_MRD&quot;</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Message is response to the message or request</td>
<td>Sample message logged in Cisco Unified EIM &amp; WIM Logs</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>START_APPLICATION_TASK_RESP</td>
<td>CTI Server responds to the START_APPLICATION_TASK_REQ message.</td>
<td>START_APPLICATION_TASK_RESP</td>
<td>Invokeld for which START_APPLICATION_TASK_RESP is received&lt;br&gt;invokeId=582&lt;br&gt;listenerInstanceId=2000</td>
</tr>
<tr>
<td>PAUSE_TASK_IND</td>
<td>Listener reports that the agent has paused the task.</td>
<td>PAUSE_TASK_IND</td>
<td>Executing PAUSE_TASK_IND for&lt;br&gt;icmAgentId=5241,&lt;br&gt;mrdId=5026,&lt;br&gt;activityId=1007,&lt;br&gt;interruptionState=0</td>
</tr>
<tr>
<td>PAUSE_TASK_EVENT</td>
<td>CTI Server acknowledges that the specified agent has temporarily suspended handling of the specified task.</td>
<td>PAUSE_TASK_IND</td>
<td>Incoming PAUSE_TASK_EVENT pooled in executor for listenerInstanceId = 2000</td>
</tr>
<tr>
<td>RESUME_TASK_IND</td>
<td>Listener reports that the agent has resumed the task.</td>
<td>RESUME_TASK_IND</td>
<td>Incoming RESUME_TASK_EVENT pooled in executor for listenerInstanceId = 2000</td>
</tr>
<tr>
<td>RESUME_TASK_EVENT</td>
<td>CTI Server acknowledges that the specified agent has resumed handling the specified task after previously sending the PAUSE_TASK_IND message.</td>
<td>RESUME_TASK_IND</td>
<td>Incoming RESUME_TASK_EVENT pooled in executor for listenerInstanceId = 2000</td>
</tr>
<tr>
<td>WRAPUP_TASK_IND</td>
<td>Listener reports that the agent has started wrap-up work for a task.</td>
<td>WRAPUP_TASK_IND</td>
<td>Send to Arm for activityId=1774 of ListenerInstance: 2000</td>
</tr>
<tr>
<td>WRAPUP_TASK_EVENT</td>
<td>CTI Server acknowledges that the specified agent is no longer actively handling the task but is doing wrap-up work related to the task.</td>
<td>WRAPUP_TASK_IND</td>
<td>Received WRAPUP_TASK_EVENT</td>
</tr>
</tbody>
</table>
### Agent Interruption Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Message is response to the message or request</th>
<th>Sample message logged in Cisco Unified EIM &amp; WIM Logs</th>
<th>Sample message logged in Unified CCE or CMB Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>END_TASK_IND</td>
<td>Listener reports that the agent has ended the task.</td>
<td>END_TASK_IND message sent to ARM</td>
<td>END_TASK_IND (InvokeId:0x5a9a, MRDId:5026, ICMAgentId:5241) 11:38:57 SESSION 3: TaskId:150167/208/5ICMDisposition:38 ApplicationDisposition:0)</td>
<td></td>
</tr>
<tr>
<td>END_TASK_EVENT</td>
<td>CTI Server acknowledges that the specified agent has finished handling the specified task.</td>
<td>END_TASK_IND received with ICMDisposition = 40 for ICMTaskId = 315_150159_13</td>
<td>END_TASK_EVENT (MonitorId:0, PeripheralId:5000, PeripheralType:DEFINITY ECS non-EAS 10:49:10 SESSION 2: MRDId:5026, ICMAgentId:5241 PreviousICMTaskId:-1/-1/-1TaskId:150167/208/3ICMDisposition:40 ApplicationDisposition:0xfffffff WrapupData:&quot;&quot; ApplicationData:&quot;&quot;)</td>
<td></td>
</tr>
<tr>
<td>AGENT_MADE_NOT_ROUTABLE_EVENT</td>
<td>CTI Server notifies Listener that the agent is made not routable for the MRD.</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>AGENT_INTERRUPT_ADVISORY_EVENT</td>
<td>CTI Server notifies Listener that the agent has been interrupted by a non-interruptible task.</td>
<td>AGENT_INTERRUPT_ACCEPTED_IND message data for AGENT_INTERRUPT_ADVISORY_EVENT event ListenerInstanceId=2000, ICMAgentId=5613, MRDId=5035, interrupting MRDId=5034, interrupting InvokeId=44187</td>
<td>AGENT_INTERRUPT_ADVISORY_EVENT (InvokeId ,MRDId, InterruptingMRDId, ICMAgentId)</td>
<td></td>
</tr>
<tr>
<td>AGENT_INTERRUPT_ACCEPTED_IND</td>
<td>Listener reports acceptance of the interrupt.</td>
<td>—</td>
<td>Sending AGENT_INTERRUPT_ACCEPTED_IND message to ARM</td>
<td>AGENT_INTERRUPT_ACCEPTED_IND (InvokeId ,MRDId ,ICMAgentId)</td>
</tr>
</tbody>
</table>

**Sample message logged in Cisco Unified EIM & WIM Logs**

- END_TASK_IND
  - InvokeId:0x5a9a
  - MRDId:5026
  - ICMAgentId:5241
  - 11:38:57 SESSION 3: TaskId:150167/208/5ICMDisposition:38
  - ApplicationDisposition:0

- END_TASK_EVENT
  - MonitorId:0
  - PeripheralId:5000
  - PeripheralType:DEFINITY ECS non-EAS
  - 10:49:10 SESSION 2: MRDId:5026
  - ICMAgentId:5241
  - PreviousICMTaskId:-1/-1/-1
  - TaskId:150167/208/3
  - ICMDisposition:40
  - ApplicationDisposition:0xfffffff
  - WrapupData:""
  - ApplicationData:""

**Sample message logged in Unified CCE or CMB Logs**

- END_TASK_IND
  - 11:38:57 SESSION 3: TaskId:150167/208/5
  - ICMDisposition:38
  - ApplicationDisposition:0

- END_TASK_EVENT
  - MonitorId:0
  - PeripheralId:5000
  - PeripheralType:DEFINITY ECS non-EAS
  - PreviousICMTaskId:-1/-1/-1
  - TaskId:150167/208/3
  - ICMDisposition:40
  - ApplicationDisposition:0xfffffff
  - WrapupData:""
  - ApplicationData:""
<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Message is response to the message or request</th>
<th>Sample message logged in Cisco Unified EIM &amp; WIM Logs</th>
<th>Sample message logged in Unified CCE or CMB Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGENT_INTERRUPT_UNACCEPTED_IND</td>
<td>Listener reports non-acceptance of the interrupt.</td>
<td>—</td>
<td>Sending AGENT_INTERRUPT_UNACCEPTED_IND message to ARM (InvokeID:0x6 MRDID:5036 ICMAgentID:5613)</td>
<td></td>
</tr>
<tr>
<td>AGENT_INTERRUPT_DONE_ADVISORY_EVENT</td>
<td>CTI Server notifies Listener that the interrupt has ended.</td>
<td>—</td>
<td>PRINT_STATE after receiving AGENT_INTERRUPT_DONE_ADVISORY_EVENT from ARM: IcmAgentID=5613 MrdId = 5034</td>
<td>AGENT_INTERRUPT_DONE_ADVISORY_EVENT (InvokeID ,MRDID ,ICMAgentID)</td>
</tr>
</tbody>
</table>

### Session Synchronization Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Message is response to the message or request</th>
<th>Sample message logged in Cisco Unified EIM &amp; WIM Logs</th>
<th>Sample message logged in Unified CCE or CMB Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEGIN_AGENT_INIT_IND</td>
<td>Listener reports that it will begin the agent and task resynchronization.</td>
<td>—</td>
<td>Sending BEGIN_AGENT_INIT_IND ()</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13:05:11 Trace: ProcessBeginAgentInitInd - sessionID 9</td>
<td>13:05:11 Trace: SendARMMsg -- SessionID = 9, ApplicationPathID = 5010</td>
</tr>
<tr>
<td>AGENT_INIT_READYEVENT</td>
<td>CTI Server notifies Listener that Unified CCE is ready to receive agent and task resynchronization messages.</td>
<td>—</td>
<td>Received AGENT_INIT_READYEVENT</td>
<td>AGENT_INIT_READYEVENT (ReadyCount:10)</td>
</tr>
<tr>
<td>AGENT_INIT_REQ</td>
<td>Listener reports the current state of the agent.</td>
<td>—</td>
<td>AgentInitReqMessage eCmd queued in messageQueue@!$ mrdId= 5028 userId= 1031 listenerInstanceID=2000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13:05:11 SESSION 9: InterruptingMRDID:0 InterruptingInvokeID:0 IsNotReady:False MaxTaskLimit:1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13:05:11 SESSION 9: AvailableDuration:1370 LogonDuration:2542 NotReadyDuration:1174 RoutableDuration:2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13:05:11 SESSION 9: NumTasks:1 AgentInfo:’ 1005’ )</td>
<td></td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Message is response to the message or request</td>
<td>Sample message logged in Cisco Unified EIM &amp; WIM Logs</td>
<td>Sample message logged in Unified CCE or CMB Logs</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>AGENT_INIT_RESP</td>
<td>CTI Server responds to the AGENT_INIT_REQ message.</td>
<td>AGENT_INIT_REQ</td>
<td>AGENT_INIT_RESP (InvokeID:0x4 ARMStatus:E_ARM_STAT_OK)</td>
<td>AGENT_INIT_RESP (InvokeID:0x4 ARMStatus:E_ARM_STAT_OK)</td>
</tr>
<tr>
<td>TASK_INIT_REQ</td>
<td>Listener report the state of the task. It is used when an Unified CCE TASKID has not yet been assigned to the task because the activity was generated when the CTI Server or Listener service was down.</td>
<td>TASK_INIT_REQ messages&gt;&gt;&gt;&gt;&gt;&gt;&gt;&gt; icmTaskId=150172_201_1 mrdId=5035 invokeId=44187 icmAgentId=5613 armSkillGroupId=5612 armServiceId=-1 paused=0 taskState=2 offerDuration=486 beginDuration=1330424236 interruptDuration=0 pauseDuration=0 wrapDuration=1330424279 appRouted=0</td>
<td>TASK_INIT_REQ (PreviousICMTaskID:-1/-1/-1MRDID:5031 InvokeID:0x71 iCMAgentID:5719 ARMSkillGroupID:N/A ARMServiceID:N/A Paused:False TaskState:1 OfferDuration:0 NumTasks:0 AgentMode:0 MaxTaskLimit:1 iCMAgentID:5057 AgentAvailabilityStatus:0 AgentID:&quot;121&quot; AgentExtension:&quot;&quot; AgentInstrument:&quot;&quot; FltSkillGroupNumber:12134 BeginDuration:0 InterruptDuration:0 PauseDuration:0 WrapupDuration:0 FltSkillGroupID:5000 FltSkillGroupPriority:0 FltSkillGroupState:LOGOUT FltSkillGroupNumber:1224 FltSkillGroupID:5019 FltSkillGroupPriority:0 ApplicationRouted:True NumNamedVariables:0 NumNamedArrays:0 FltSkillGroupState:LOGOUT )</td>
<td>TASK_INIT_REQ (PreviousICMTaskID:-1/-1/-1MRDID:5031 InvokeID:0x71 iCMAgentID:5719 ARMSkillGroupID:N/A ARMServiceID:N/A Paused:False TaskState:1 OfferDuration:0 NumTasks:0 AgentMode:0 MaxTaskLimit:1 iCMAgentID:5057 AgentAvailabilityStatus:0 AgentID:&quot;121&quot; AgentExtension:&quot;&quot; AgentInstrument:&quot;&quot; FltSkillGroupNumber:12134 BeginDuration:0 InterruptDuration:0 PauseDuration:0 WrapupDuration:0 FltSkillGroupID:5000 FltSkillGroupPriority:0 FltSkillGroupState:LOGOUT FltSkillGroupNumber:1224 FltSkillGroupID:5019 FltSkillGroupPriority:0 ApplicationRouted:True NumNamedVariables:0 NumNamedArrays:0 FltSkillGroupState:LOGOUT )</td>
</tr>
</tbody>
</table>
UI Debugging Tools

There are five debugging tools available. They are:

- F12 Developer Tools (page 37)
- UI Logging Utility (page 38)
- Fiddler and HttpWatch (page 40)
- Cisco Unified Web and E-Mail Interaction Manager Debugger (page 41)
- Java Debugging (page 42)

F12 Developer Tools

IE Developer Tools allow you to debug client side and server side scripts.

Script debugging is turned off by default in Internet Explorer. Enable this tool when you see script errors while using the application. Once the tool is on, every time you see a script error, you are given an option to debug the problem. If you select the option, the tool points you to the exact line that is causing the problem in the code.

To enable the F12 developer tools in Internet Explorer:

1. Close all open Internet Explorer browser windows.
2. Restart Internet Explorer.
3. From the menu, select Tools > Internet Options.
4. In the Internet Options window, on the Advanced tab, go to the Browsing section. Make the following changes:
   a. Clear the Disable script debugging (Internet Explorer) option.
   b. Clear the Disable script debugging (Other) option.

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Message is response to the message or request</th>
<th>Sample message logged in Cisco Unified EIM &amp; WIM Logs</th>
<th>Sample message logged in Unified CCE or CMB Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>TASK_INIT_RESP</td>
<td>CTI Server responds to the TASK_INIT_REQ message.</td>
<td>TASK_INIT_REQ</td>
<td>Received TASK_INIT_RESP</td>
<td>TASK_INIT_RESP (InvokeID:0x71 \n ARMStatus:E_ARM_STAT_OK TaskID:150175/59627100/0)</td>
</tr>
</tbody>
</table>
| END_AGENT_INIT_IN_D   | Listener reports the end of agent and task resynchronization. | —                                              | Sending END_AGENT_INIT_IN_D                           | END_AGENT_INIT_IND () 13:05:11 Trace: SkTgtID=5241  
 SkGrpNo=0x659  
 SkGrpID=5234 NumLines=0  
 CurLine=-1 ClientStatus=0x1 |
c. Select the **Display notification about every script error** option.

5. Close Internet Explorer.

6. Launch Internet Explorer and launch the application.

**Request Response Data and UI Logging Utility**

**About the Utility**

The **Request Response Data and UI Logging Utility** is used to capture the application’s UI code flow. It also captures details of requests sent to the server and the corresponding responses sent from the server. The utility is used for troubleshooting issues related to the following user experiences:

- The application gets stuck on an hourglass cursor.
- Javascript errors while accessing certain parts of the application.
- Application non-responsiveness when attempting an action.
- General slowness of the application.

When running the utility, logging begins instantly and users do not need to log out and log in. Logging ends when the time frame specified in the utility has elapsed. To record the log details beyond the specified time frame, a partition administrator must re-configure and enable logging using the utility. If the system is restarted during the logging process, the logging stops and you must reconfigure and rerun the utility from the Tools Console. If there is a need to debug static content, such as html and javascript files, tools such as **Fiddler** or **HttpWatch** may be required.

**Log Files**

This utility generates two log files. Both files can be found at the following location: 
Cisco_Home\eService\logs. Each log file records data for all the specified users.

- **UI Logs**: These logs record details on the code flow of all the application’s consoles except the Offers Console. The UI utility generates a log file with the name: `eg_log_ui_data_Application_Server.log`.

- **Request Response Data Logs**: This log records response data for requests that come to the application server, as well as the corresponding responses sent from the server. Data generated in these log files include: URI, request parameters, session ID, cookies, request headers, response content, and time taken in processing a request. The log file is generated with the name: `eg_log_request_response_data_Application_Server.log`.

**Logging Utility Options**

These are the logging options available when running the utility.

- **Log the response text for all the requests**: Checking this box allows the utility to capture the application server’s response text when it responds to requests sent to the server.

- **Enable logging**: Activates the utility. Logging must be enabled before user IDs and URLs can be added for logging.
Please note that if the application has multiple application servers and is being accessed through a load balancer, running the utility enables logging for the specified users on all of the application servers. Thus, a user with logging enabled can log out from one application server and log in on another application server. The logs are captured for each server the user logged into without need for reconfiguring the logging utility.

- **Disable logging:** Ends the logging process.
- **Add user for logging:** Specify a user for data capture. Separate multiple users with commas. White spaces are ignored. Users with white space in their ID cannot be logged.
- **Remove user from logging:** Stops logging for the specified user. Separate multiple users with commas.
- **Add URLs for logging:** By default, all URLs in the application are logged. Specify a URL to capture data on a particular location. Separate multiple URLs with commas. Deployments with load balancers should use a sub-string of the URL, such as http://Web_Server_Name/system/web/controller/platform/admin/department/createdepartment.jsp.
- **Remove URLs for logging:** Excludes the specified URLs from the logging process. The following URLs are always excluded from logging and do not need to be excluded: getattachmentsurl.jsp, showattachment.jsp, and showreportcontent.jsp. Examples include: http://Web_Server_Name/system/web/controller/platform/admin/user/edituser.jsp
- **Remove all users and URLs from logging:** Ends logging for all users and URLs.

**To Troubleshoot With the Request Response Data and UI Logging Utility**

The Utility is available in the Tools Console of the application in the Utilities window. To troubleshoot, determine the issue users are experiencing and proceed through the associated steps. The tool cannot be run without specifying users. Multiple IDs and URLs must be separated by commas. White spaces are ignored.

**The application becomes stuck on an hourglass cursor**

1. Launch the application and log in to the Tools Console.
2. Open the Utilities window.
3. Select the Go button for Request Response Data and UI Logging Utility.
4. Set the duration and enable logging.
5. Add the IDs for the user or set of users that are experiencing the issue.
6. Reproduce the issue by performing the actions leading up to the issue.
7. If the issue is intermittent, keep logging enabled until the issue has been replicated.
8. Capture the issue with a screen shot of the UI and include a timestamp and any relevant log files.
9. Once logging is complete, collect and send relevant images and log files.

**A Javascript error is displayed**

1. See “The application becomes stuck on an hourglass cursor” on page 39.

**The application does not respond when the user attempts to perform certain actions**

1. Launch the application and log in to the Tools Console.
2. Open the Utilities window.
3. Select the Go button for Request Response Data and UI Logging Utility.
4. Set the duration and enable logging.
5. Add the URL address or addresses with which the users experience the issue.
6. Reproduce the issue by performing the actions leading up to the issue.
7. If the issue is intermittent, keep logging enabled until the issue has been replicated.
8. Capture the issue with a screen shot of the UI and include a timestamp and any relevant log files.
9. Once logging is complete, collect and send relevant images and log files.

**The application is unusually slow**
1. Launch the application and log in to the Tools Console.
2. Open the Utilities window.
3. Select the Go button for Request Response Data and UI Logging Utility.
4. Set the duration and enable logging.
5. Add the IDs of users experiencing the application’s sluggish behavior.
6. If the issue is intermittent, keep logging enabled until the issue has been replicated.
7. Once logging is complete, collect web server and application server access logs.
8. Record and send Request Response Data and UI Logging Utility files, along with any relevant web server and application server access logs.

**Fiddler or HttpWatch**

These tools can be used to gather HTTP trace on user desktops.

**HttpWatch:** This tool can be used for seamless monitoring and logging of the HTTP and HTTPS traffic from the user’s browser. There is a free version that can be used to capture information on the Customer Console. To view the details of the requests, responses etc., use the professional version.

**Fiddler:** Fiddler is a Web Debugging Proxy which logs all HTTP and HTTPS traffic between your computer and the Internet. It monitors all traffic from the desktop and not specific requests from a Unified EIM and WIM browser instance.

Both these tools can help you see:

- Real-time page and request level time charts showing performance bottlenecks.
- Low-level HTTP information such as headers, cookies, etc and millisecond accurate timings.
- The request parameters such as get and post.
- The response from the server.

**To Troubleshoot With Fiddler or HttpWatch:**
1. Download and install Fiddler or HttpWatch on the desktop where the issues are occurring.
2. Launch Internet Explorer and keep HttpWatch running for the browser instance. If you are using Fiddler, start Fiddler.

3. Access the application and recreate the issue.

4. The tools log all the requests that are being sent to the server. Analyze the output generated by these tools and look for following issues:
   a. Check for aborted 4XX, or 5XX requests for JSP or JS.
   b. Check for any network connection errors.
   c. Check the total time taken by JSP requests to fetch data from server.

5. After the issue is replicated, save the HTTP request trace to a file.

Cisco Unified Web and E-Mail Interaction Manager Debugger

The Cisco Unified Web and E-Mail Interaction Manager Debugger helps you debug the application when it hangs, or when the hour-glass cursor appears. Use this tool with F12 Developer Tools

These are some important commands in the debugger:

- **Trace On**: Enables the tracing for all the jsp and servlet requests submitted from the User Interface (UI) framework.
- **Trace Off**: Turns off the request tracing.
- **Clear Trace**: Clears the generated trace.
- **Action Trace On**: Enables the tracing of all the logical action being submitted from the framework (Example of an action is selecting an email in the inbox which involves loading the reply, updating the information pane, fetching bookmarks, etc).
- **Action Trace Off**: Turns off the tracing of actions.
- **WaitandCall Trace On**: Lists all the WaitAndCall (Javascript function that waits for a condition to be met and then triggers a call to another javascript method) calls being executed in the UI framework. This is useful to see if there is any Javascript WaitAndCall that is getting executed infinitely.
- **WaitandCall Trace Off**: Turns off the WaitandCall tracing.
- **Display Page State**: Displays the loading state of the view file (notloaded/loading/complete).
- **Display loaded applets**: Displays the number of applets in a displayed view and the number of loaded applets.
- **Timer On**: Displays the time taken for each of the jsp/servlet requests in the timer window frame. Choose Display Timer Log in the Timer log drop down menu to view the logs.
- **Timer Off**: Turns off the time logging for requests.
- **View Client Cache**: Lists all the cached objects in the local Javascript cache. For example:
  - name=dateFormat value=mm/dd/yyyy
  - name=timeFormat value=h:mm:ss a
  - name=timeZone value=Asia/Calcutta
To Troubleshoot with the Cisco Unified Web and E-Mail Interaction Manager Debugger:

1. Launch the application and log in to the console that is experiencing the problem.
2. Press CTRL + SHIFT + W to launch the debugger.
3. In the debugger window, configure the following options.
   a. Select the debug command. If you choose the Select=> option, choose a command from the dropdown list. If you select the Type=> option, then provide the name of the object and operation you want to debug. The most useful debug commands are:
      - Trace On
      - Set Default Cursor
      - Launch Global Debugger
   b. In the Timer log field, select the option to hide or display the timer log.
4. Click the Run button to start debugging.

Java Debugging

This section only applies to Knowledge Dashboards and Workflows in the Administration Console.

There are two different ways to capture Java logs:

- Through the client's file system
- Through the Java Console

Enabling the Java Console

The Java Console provides useful information about issues related to the applets. This is a useful tool when debugging issues related to Workflows in the Administration Console that use applets.

To enable the Java Console:

1. Go to Start > Control Panel.
2. Double-click on Java.
3. In the Java Control Panel window, go to the Advanced tab and make the following changes:
   a. In the Java console section, select Hide console
To enable advanced logging for the Java client:

1. On the client machine, go to **Start > Settings > Control Panel > Java** to open the Java Control Panel.
2. In the **Advanced** tab, expand the **Debugging** node and configure the following options:
   a. Select the checkbox for **Enable tracing**.
   b. Select the checkbox for **Enable logging**.
   c. Select the checkbox for **Show applet lifecycle exceptions**.

Capturing Logs from the Java Console

**To capture logs from the Java Console:**

1. Expand the taskbar menu.
2. Right-click on the Java logo.
3. Click **Open [version_number] console**
4. Press **CTRL + A** to select all the data in the window.
5. Click **Copy**.
6. Paste this data in a text file.

Capturing Java Logs From the File System

The logs from Java Console window can only be captured as long as the applet is loaded in the browser. Once the user logs out of or exits the application the Java Console window is not accessible.

**To capture logs from the file system:**

- The client Java logs may be retrieved from the following location in the client machine: `C:\Documents and Settings\<user>\ApplicationData\Sun\Java\Deployment\log` where `<user>` is the user name used to log in into the client machine.

Server Debugging Tools

Generating Thread Dumps and Heap Dumps

**About Thread Dumps**

Thread dumps are log files used to identify issues related to non-functional processes and abnormally high CPU usage by creating a record containing information on currently running threads within a process. A thread dump can be used to troubleshoot issues with the following symptoms:
A process hangs or freezes.

The system’s CPU usage is abnormally high.

A process continues running but does not perform its function. For example, a retriever process that is not retrieving emails sent to the department alias.

Thread dumps can be generated using the Unified EIM & WIM Thread Dump Utility. Please note that thread dumps should not be used unless at the request of Cisco TAC.

**About Heap Dumps**

If an issue is tied to memory, as with a memory leak, a heap dump can be used for diagnosing the problem. A heap dump is a snapshot of the memory of a Java process at a certain point in time, recording information on the objects in the process at the time the heap dump is triggered. Heap dumps are used to troubleshoot issues with the following symptoms:

- The process is using abnormally high amounts of memory on the system.
- A process becomes non-functional and generates an `OutOfMemoryError` in its log file. For example, the dispatcher process does not send an email and crashes.

Heap dumps are automatically generated when any of the application’s processes goes into an `OutOfMemoryError` state. The log file is generated in a `Java_pid_process_ID.hprof` file.

**About the Thread Dump Utility**

The Unified EIM & WIM application possesses a utility that generates thread dump log files for processes. It can be found in the Utilities section of the Tools console.

**Thread Dump Utility Configuration**

To configure settings for thread dumps, access the system partition and open the Administration Console. Configure the following partition settings:

- **Time between three successive thread dumps (milliseconds)**: When a thread dump is taken, three snapshots are used to generate one thread dump. This setting determines the time interval, in milliseconds, between each snapshot. The default value is 2000.

- **Time between thread runs (milliseconds)**: This setting determines the time interval, in milliseconds, between each logged thread dump. The default value is 3000.

- **Thread dump max stack trace**: Maximum depth of stack trace to log for each thread in a thread dump. The default value is 10.

- **Maximum number of dumps**: The maximum number of dumps to be logged for on-demand thread dump utility. The default value is 10.

**Creating a Thread Dump**

1. Determine the process that is causing the issue.
2. Find the log file of the process that’s having issues and retrieve the process ID (also known as JVM ID).
3. Access the Tools Console, open the Utilities section, and run **Dump running threads for a process**.

4. In the field labeled **ID of the Java Virtual Machine (JVM)**, enter the process ID.

5. Wait a few minutes for all thread dumps to finish logging.

6. Depending on the process logged, go to the server that the process is located on and access that process’ log file. For example, if you are recording the retriever service, you would access the services server and open Cisco_Home\eService\logs\eg_log_Services_Server_Name_rx-process.log.

7. Send the log file to Cisco TAC for further analysis.

---

**Viewing Attachments Stored in Database**

As part of troubleshooting attachments related issues, if you need to view the attachments stored in the database tables, you can do so by using the Read Attachment Utility available in the following folder: Cisco_Home\Utilities\attachments. The utility will extract the attachment from the database to the location specified while configuring the utility.

To be able to run this utility, you need the following information:

- A location where you want to extract the attachments.
- The type of object for which you are extracting the attachment. It can be: KB, Mail, Task, Other
- The ID of the object for which you want to extract the attachments.

**To configure the utility:**

- On the file server, open the Cisco_Home\Utilities\attachments\readAttachmentsUtility.bat file in a text editor and edit the following properties.
  
  - Locate the 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, C:\Java\jdk1.7.0_02.
  
  - Locate the SET PL_HOME_LOCAL property and set the value to the location where Unified EIM and WIM is installed. For example, C:\Cisco\eService.

**To run the utility:**

- Run the following command to launch the utility.

  readAttachmentUtility.bat Attachment_ID Object_Type Location_For_Attachment

  For example: readAttachmentUtility.bat 1000 Mail D:\attachments

The utility extracts the attachments from the database and stores them to the location provided while running the utility.
5 General Issues

- Installation Issues
- Application Start-up Issues
- Logging In Issues
- Login Issues
- Logout Issues
- User Interface Issues
Installation Issues

About Installation Logs

Logs generated during the installation process are typically created in the following location:

Cisco_Home\eService\installation\logs

- If the installer fails to detect the file system, the log file, egain_installer_server_name.log, is created in the following location: C:\Users\Your_Username\AppData\Local\Temp. You may also access this location with a %TEMP% shortcut.

Symptom 1: “Unable to Connect to Database” Error During Installation

The Unified EIM and WIM installation program shows an “Unable to Connect to Database” error even when the database details provided on the database parameters screens are correct. Check the installation log file:

- If file server is already installed:
  Cisco_Home\eService\installation\logs\eg_log_Server_Name_egainInstaller.log

- If it is a new installation:
  C:\Users\Your_Username\AppData\Local\Temp\egain_installer_Server_Name.log.

In the log file, look for the following error message:

A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections.

Cause 1: SQL Server Service Not Running

The SQL server service is not running on the database machines.

**Recommended actions:**

1. Go to Start > All Programs > Administrative Tools > Services.
2. Ensure that the SQL server service is running.

Cause 2: TCP/IP Protocol is Disabled

The TCP/IP protocol has not been enabled on the database machines.

**Recommended actions:**

1. Go to Start > All Programs > Microsoft SQL Server 2012 > Configuration Tools > SQL Server Configuration Manager.
2. In the SQL Server Configuration Manager window, browse to SQL Server Network Configuration > Protocols for InstanceName. If you specified the default instance during installation, the instance name will be MSSQLSERVER.
3. Verify that **TCP/IP** is enabled. If it is not enabled, right-click **TCP/IP** and from the drop-down menu, select **Enable**.

![Enable TCP/IP](image)

**Cause 3: TCP Port Blocked by Firewall**

The TCP port is getting blocked by the firewall.

**Recommended actions:**

1. Go to **Start > All Programs > Microsoft SQL Server 2012 > Configuration Tools > SQL Server Configuration Manager.**

2. In the SQL Server Configuration Manager window, browse to **SQL Server Network Configuration > Protocols for InstanceName.** If you specified the default instance during installation, the instance name will be **MSSQLSERVER.**

3. Right-click **TCP/IP** and from the drop-down menu select **Properties.**
4. In the TCP/IP Properties window, from the IP Addresses tab note down the **TCP Port**.

![TCP/IP Properties](image)

*Note down the TCP Port*

5. Check the Windows firewall settings to make sure that this TCP port is not blocked by the firewall.

---

**Symptom 2: “Unable to Create Database” Error During Installation**

The Unified EIM and WIM installation fails and the following error message is displayed: **Unable to create database.**

**Cause 1: Not Enough Space Available on Database Machine**

There is not enough disk space available on the database machines to install the Unified EIM and WIM databases.

**Recommended actions:**

1. Check the log file  
   `Cisco_Home\eService\installation\eg_log_Server_Name_eGainInstaller.log` for the message recorded while running the installer. The message will be in the following format:
   
   `********** Exception while creating the database **********`  
   error message recorded by the installer.

2. Check the database machines and ensure that there is ample disk space available for creating data and log files for the Unified EIM and WIM databases.
Cause 2: Correct Permissions Not Assigned to Database Administrator User

The database administrator user created for installing Unified EIM and WIM has not been assigned the required roles and permissions. This problem will be generally seen by people who are not using the default database administrator user for installing the application.

Recommended actions:

1. Check the log file
   
   Cisco_Home\eService\installation\eg_log_Server_Name_eGainInstaller.log for the message recorded while running the installer. The message will be in the following format:
   
   ******* Exception while creating the database **********
   
   error message recorded by the installer.

2. Check the database schema log files for messages starting with Error Message.
   
   Cisco_Home\eService\installation\logs\egpl_dbSchema_oracle.log

3. If the log messages suggest that the database administrator user does not have the correct permissions or roles, reassign the permissions and roles and try to install the application again. For details on the permissions or roles required for the user, see the Cisco Unified Web and E-Mail Interaction Manager Installation Guide.

Symptom 3: Unable to Start the Unified EIM and WIM Windows Service

When the Cisco Service is started from the Windows Service panel, the following error message is displayed:

Could not start the Cisco Service on Local computer. Error 1069: The service did not start due to logon failure.

Cause: Incorrect Domain User Name and Password Information

Incorrect domain username or password was provided while installing the Unified EIM and WIM.

Recommended actions:

1. On the machine where you are unable to start the application, access the Windows Services panel and do the following:
   
   a. Right-click the Cisco Service and select Properties.

   b. In the Cisco Service Properties window go to the Log On tab and provide the account username and password again.
c. Save the changes by clicking the **OK** button.

![Cisco Service Properties](image)

*Change the log on parameters*

2. Start the Cisco Service.

**Symptom 4: Unable to Run the Unified EIM and WIM Upgrade Installer**

Upgrade installer does not list installed components correctly in the Product Information window.

**Cause 1: Application Server Not Listed in Product Information Window**

While running the upgrade installer on the application server, the upgrade installer does not identify the application server installed on that machine. The Product Information window shows the list of components installed on that server, but it does not list the application server.

This issue occurs if the correct application server is not recorded in the master database.

**Recommended actions:**

1. Run the following query on the Unified EIM and WIM master database:
   
   ```sql
   select host_name, url, description from egpl_dsm_host
   ```

2. In the query results, check the value of the **host_name** column for the application servers. The values should match the names of the application servers in your deployment.

3. If the values do not match, collect all the logs from the `Cisco_Home\eService\logs` folder and share the log files with Cisco TAC for further analysis.
Cause 2: Messaging Server Not Listed in Product Information Window

While running the upgrade installer on the messaging server, the upgrade installer does not identify the messaging server installed on that machine. The Product Information window shows the list of components installed on that server, but it does not list the messaging server.

This issue occurs if the correct messaging server is not recorded in the master database.

Recommended actions:

1. Run the following query on the Cisco master database:
   
   ```sql
   select host_name, url, description from egpl_dsm_host
   ```

2. In the query results, check the value of the `host_name` column for the messaging servers. The values should match the names of the messaging servers in your deployment.

3. If the values do not match, collect all the logs from the `Cisco_Home\eService\logs` folder and share the log files with Cisco TAC for further analysis.

Cause 3: Services Server Not Listed in Product Information Window

While running the upgrade installer on the services server, the upgrade installer does not identify the services server installed on that machine. The Product Information window shows the list of components installed on that server, but it does not list the services server.

This issue occurs if the correct value of the services server is not recorded in the master database.

Recommended actions:

1. Run the following query on the Unified EIM and WIM master database:
   
   ```sql
   select host_name, url, description from egpl_dsm_host
   ```

2. In the query results check the value of the `host_name` column for the following:
   - Host Controller
   - DSM Controller
   - RMI Registry Server
   - RMID Registry Server

   The value should match the services server name.

3. If the value is not correct, collect all the logs from the `Cisco_Home\eService\logs` folder and share the log files with Cisco TAC for further analysis.

Cause 4: Web Server Not Listed in Product Information Window

While running the upgrade installer on the web server, the upgrade installer does not identify the web server installed on that machine. The Product Information window shows the list of components installed on that server, but it does not list the web server.

This issue occurs if the correct value of the web server is not recorded in the master database.
Recommended actions:

1. Run the following query on the Unified EIM and WIM master database:
   
   ```sql
   select host_name, url, description from egpl_dsm_host
   ```

2. In the query results check the value of the `host_name` column for the web server.
   The value should match the web server name.

3. If the value is not correct, collect all the logs from the `Cisco_Home\eService\logs` folder and share the log files with Cisco TAC for further analysis.

Symptom 5: “Access Denied” Error While Running Upgrade Installer

Upgrade installer fails while copying the installation files in the installation folder. The following error occurs: *Access Denied*.

**Cause 1: Files Under the File Server Installation Folder are Read-Only**

**Recommended actions:**

1. Run the following command on the installation folder and get attributes of all files. Ensure that the files are not marked read-only.
   
   ```cmd
   attrib /D /S *
   ```

2. If there are read only files, change the attributes of the file by executing the following command on the installation folder:
   
   ```cmd
   attrib /D /S * -R
   ```

**Cause 2: Files Under the File Server Installation Folder are In Use**

This issue can occur if the application is still running, or if some of the files from the installation folder are open in a text editor.

**Recommended actions:**

1. Check if the application is running. If it is running, stop the application.

2. Check if there are any files open from the installation folder and close them.

3. Try to run the upgrade installer.

Application Start-up Issues

**Symptom: Application Not Starting on All servers**

In a distributed server installation, the application starts on some servers and not others. As a result, users are not able to access the application.
Cause 1: Required Ports Not Available

Certain ports should be open between the application’s components for communication. If the required ports are not open or they are in use by some other application, then the Unified EIM and WIM application will not start. In the log files available at `Cisco_Home\eService\logs` you will see log messages like “SocketException”.

**Recommended actions:**
1. Refer to the *Cisco Unified Web and E-Mail Interaction Manager Deployment and Maintenance Guide* for details about the ports which need to be open between the various components.
2. On the file server, check the following file to see the current ports configured for the installation:
   ```bash
   Cisco_home\eService\bin\platform\windows\setenv_ServerName.bat
   ```
3. If the ports are being used by another application, you will need to assign a different port to those applications.

Cause 2: All Unified EIM & WIM Components Not Updated to Same Version

The application will not start if all Unified EIM and WIM components are not updated to the same version. For example, if you apply 11.0.1 to the file server and not to the web server, the application will not start.

The log files `Cisco_Home\eService\installation\logs\egpl_root_ServerName.log` and `Cisco_Home\eService\installation\logs\eg_log_ServerName_misc.log` will have messages like “FATAL[ServerUpdateStatus, main]: Unable to start Application *****”

**Recommended actions:**
1. Run the following query on the master database to check which components are not updated:
   ```sql
   SELECT HOST_NAME, RELEASE_VERSION FROM EGPL_DSM_HOST
   ```
2. Run the Update installation program to update all the components to the same version.
3. Starting the application to see if the problem is fixed.
4. If you ran the update installer and the entries in the master database table are still not updated, then contact Cisco TAC support along with the following log files:
   - `Cisco_Home\eService\installation\logs\egpl_root_ServerName.log`
   - `Cisco_Home\eService\installation\logs\eg_log_ServerName_misc.log`

Cause 3: Low Disk Space

EAR is not getting deployed because there is not enough disk space on the drive where JBoss is installed. EAR is extracted in the `temp` folder so the disk should have space more than the size of the EAR.

**Recommended actions:**
- Follow the sizing guidelines in the *Cisco Unified Web and E-Mail Interaction Manager Deployment and Maintenance Guide* to make sure that your hardware meets the requirements defined in the guide.
**Cause 4: EAR Deployment Timed Out**

If EAR is not deployed in the specified time (default is 500 seconds), then JBoss marks the deployment as timed out (failed). A file `eService.ear.failed` is created at: `JBoss_Home/standalone/deployments`. If this is the problem, then this file will have an error similar to “JBAS015052: Did not receive a response to the deployment operation within the allowed timeout period [500 seconds].”

This can occur if the machine is busy or too slow.

**Recommended actions:**

- Make sure that the hardware used for the installation meets the sizing guidelines provided in the *Cisco Unified Web and E-mail Interaction Manager Deployment and Maintenance Guide*. If the hardware meets the requirements defined in the guide and you are still running into this issue, then contact Cisco TAC.

**Logging In Issues**

**Symptom 1: 404 Error Page Displayed While Logging In**

Users accessing the application URL receive a 404 error page instead of the login page.
Cause: Context Root Name in the URL is Incorrect

Make sure that you are using the correct context root name in the URL. Also note that the context root name is case sensitive and should exactly match the name provided at the time of installation.

For example, if the context root name is CompanyName the URL should be "http://Server_Name/CompanyName/web/view/platform/common/login/root.jsp?partitionId=1"

Recommended actions:

1. Run the following query on the active database to get the exact name of the context root used for the application:

   SELECT VALUE FROM EGPL_CONFIG_PROPERTY WHERE NAME = 'eservice.module.context'

2. Note down the correct context root name and try accessing the application with the correct link.

Symptom 2: Internal Server Error Page Displayed While Logging In

When the user accesses the application URL, they receive an internal server error page instead of the login page.

The error displayed is:

   Internal server error.
   There is a problem with the resource you are looking for and it cannot be displayed.

Cause: Permissions Not Assigned for egain-plugin Folder

The installation program automatically configures folder permissions at the time of installation. If these permissions are changed at a later point, the application will become inaccessible.

Recommended actions:

1. On the web server, browse to Cisco_Home\eService\Installation
2. Right-click the egain-plugin folder and from the menu select Properties.
3. In the egain-plugin Properties window, go to the Security tab and click the Edit button.
4. In the Permissions for egain-plugin window, click the Add button.
5. In the Select Users or Groups window, click the Locations button.
6. In the Locations window, select the web server name and click OK.

![Select the web server](select_web_server.png)

7. In the Select Users or Groups window, in the Enter the object name to select field, add DefaultAppPool.

![Enter the object name](enter_object_name.png)

8. Give full access to the newly added user DefaultAppPool.
9. Try accessing the application again to see if the problem is fixed.

**Symptom 3: Internet Explorer Cannot Display Webpage When Logging In**

The application is running and the EAR is deployed properly, but the user is still unable to access the application. The following error message is displayed when the user tries to log into the application:

*Internet Explorer Cannot Display the Webpage*

**Cause: Web Server Not Running**

Application will not be accessible if IIS (Internet Information Server) is not running on the web server. To check if IIS is running, access the default page of the web server: `http://Web_Server_Name`. If you get an error page, you need to start the IIS.

**Recommended actions:**

- To start the IIS, go to the Windows Services panel and start the **World Wide Web Publishing Service**. From the Internet Information Services (IIS) manager, verify that the website used by the application is also started.
Login Issues

Overview

When a mapped agent logs into the Agent Console, the agent is authenticated in both Unified EIM and WIM and Unified CCE for all MRDs that the agent is associated with in Unified CCE. This ensures that once logged in, the agent can work on mail and chat activities routed by Unified CCE from a single unified Agent Console.

This section describes the various issues that can occur at the time of login.

Symptom 1: “Login Not Successful to One or More MRDs” Error Message

The following error message is displayed to agents while logging in to Unified EIM and WIM and they are not able to log in to the application.

Login was not successful for one or more media routing domains. Please contact your administrator for verification of agent configuration in Unified EIM & WIM and Unified CCE.

Cause: MRD Missing From Application Path Member List

An agent can be configured for multiple MRDs in Unified CCE. When an agent logs in through the Agent Console, the MEDIA_LOGIN_REQ message is sent for every configured MRD to Unified CCE through the Listener service. Each of these MEDIA_LOGIN_REQ messages should have a valid response for an agent to be able to login successfully. The MEDIA_LOGIN_RESP message returned with a failure for any of the MRDs will result in login failure.

Recommended actions:

1. Get the CTI server logs for the time at which the agent login failed. The MEDIA_LOGIN_RESP message will be observed with an appropriate ARMStatus message. The message in the log file will look like this:

   `MsgType:MEDIA_LOGIN_RESP (InvokeId:0x24bb
   ARMStatus:E_ARM_STAT_LOGIN_NOT_ALLOWED_FOR_APP_PATH)`

2. From the Unified CCE Configuration Manager check that the MRDs for all agents who are supposed to log in to Unified EIM and WIM are associated as Application Path Members to the Application Instance with which Unified EIM and WIM is integrated. For details on configuring these objects, see the Cisco Unified Web and E-Mail Interaction Manager Deployment and Maintenance Guide.

Symptom 2: “Login timed out with Unified CCE” Error Displayed on Login

The following error message is displayed to agents while logging in to Unified EIM and WIM and they are not able to log in to the application.

Login timed out with Unified CCE. Please contact your administrator for verification of CTI server status, CMB connectivity, network connectivity or latency for Unified CCE connections, and running state of Listener process and instance in Unified EIM & WIM. Also ensure there are email and chat licenses available for this agent to use for login.
**Cause 1: Listener Service Process or Instance Not Running**

**Recommended action:**
- From the System Console, ensure that the Listener service process and instance are running. Start them if required.

**Cause 2: Media_Login_Resp Message Not Returned Within Timeout Interval**

The Unified EIM and WIM login screen is designed to complete agent login within the configured timeout settings. If the responses from Unified CCE for `MEDIA_LOGIN_REQ` are delayed, the agent login is terminated in Unified EIM and WIM and the agent is not allowed to log in to the Agent Console.

This feature is governed by the `LISTENER_MAX_LOGIN_WAIT_TIME_IN_MILLISEC` property available in the active database. The default value of this property is 30 seconds. Run the following query to find the value of the property:

```
SELECT VALUE FROM EGPL_CONFIG_PROPERTY WHERE NAME = 'LISTENER_MAX_LOGIN_WAIT_TIME_IN_MILLISECS' AND DOMAIN = 'ipcc.egicm_configuration.properties'
```

**Recommended actions:**
1. From the System Console, set the logging level for the Listener-process to INFO level. This level is required to view the messages the Listener service sends to ARM.
2. After changing the log levels, check the `Cisco_Home\eService\logs\eg_log_Services_Server_Name_Listener-process.log` file. Verify that the `MEDIA_LOGIN_REQ` message is sent for all configured MRDs to Unified CCE.
3. After the login time out failure message is seen by the agents, verify that a logout is triggered and the `MEDIA_LOGOUT_IND` message is sent for each MRD to Unified CCE to terminate the login. Check the `Cisco_Home\eService\logs\eg_log_Services_Server_Name_Listener-process.log` file. Here you see all `MEDIA_LOGOUT_IND` messages going to Unified CCE.
4. If the agents are continuously seeing the error message at the time of login, increase the value of the `LISTENER_MAX_LOGIN_WAIT_TIME_IN_MILLISEC` property in the `EGPL_CONFIG_PROPERTY` table of the active database.

   Use the following query to update it:

   ```
   UPDATE EGPL_CONFIG_PROPERTY SET VALUE = Time WHERE NAME = 'LISTENER_MAX_LOGIN_WAIT_TIME_IN_MILLISECS' AND DOMAIN = 'ipcc.egicm_configuration.properties'
   ```

**Further actions:**
If none of the above mentioned recommended actions solve your problem, then collect the following information and send it to Cisco TAC.
- From the Unified EIM and WIM services server:
  - `Cisco_Home\eService\logs\eg_log_Services_Server_Name_Listener-process.log`
  - `Cisco_Home\eService\logs\eg_log_Application_Server_Name_ApplicationServer.log`
- CTI server logs.
Symptom 3: “Log Out Now” Error Message Displayed on Login

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

The following error message is displayed to agents while logging in to Unified EIM & WIM and they are not able to log in to the application:

This action could not be completed due to a delay with the server. You will need to log out and log back in again.

If you were working in a text editor and have not saved your work, please copy it into another program and then click the Log Out Now button.

Cause 1: Primary Unified CCE AW Database Not Configured Correctly

If the deployment only has a primary Unified CCE Administration Workstation Database (AWDB) and the database is not running or not configured properly, this issue can occur.

Recommended actions:

1. Check the application server log file for errors. The “DBConnectionException” log message is recorded in the Cisco_Home\eService\logs\eg_log_Appliedation_Server_Name_ApplicationServer.log file when this issue occurs. The log message appears as:
   com.egain.platform.framework.dataaccess.exception.DBConnectionException: SQLState=08S01|SQLException is:The TCP/IP connection to the host ggns38, port 1433 has failed. Error. "connect timed out. Verify the connection properties, check that an instance of SQL Server is running."

2. Ensure that the primary Unified CCE AWDB database is up and running. Go to the database machine and from the Windows Service panel check if the SQL Server Agent and MSSQL services are running.

3. In the system partition (zero partition), go to the System Console and verify that the database properties are configured correctly. For details, see the “Configuring Database Details” section of the Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to System Console.

Cause 2: Secondary Unified CCE AW Database Not Configured Correctly

If the deployment has a primary and secondary Unified CCE Administration Workstation Database (AWDB), and the primary database server becomes unavailable, the application is unable to connect to the secondary database if the secondary database is not running or is not configured properly.

Recommended actions:

1. Check the application server log file for errors. The primary and secondary AWDB connection failure log messages are recorded in the Cisco_Home\eService\logs\eg_log_Appliedation_Server_Name_appliedationserver.log file when this issue occurs. Notice the host names in the logs (host AWDB machine). There will be one stack trace from the primary AWDB and another for the secondary AWDB when the application tries to rollover from the primary to secondary connection pools and fails. Logs indicating the rollover from the primary to the secondary database are also displayed.

The log message appears as:

w2012-03-27 17:10:50.417 GMT+0530 <@> ERROR <@> [8241:RMI TCP Connection(11342)- 10.10.61.62] <@> ProcessId:7040 <@> PID:1 <@> UID:12
2. Ensure that the secondary Unified CCE AWDB database is up and running. Go to the database machine and from the Windows Service panel check if the SQL Server Agent and MSSQL services are running.

3. In the System partition, go to the System Console and verify that the database properties are configured correctly. For details, see the “Configuring Database Details” section of the Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to System Console.

**Cause 3: Unified CCE AW Database Connection Pool Limit Exceeded**

There is a limit to the number of connections that can be made to the Unified CCE AWDB. If this limit exceeds the configured limit, the JDBC calls to the Unified CCE AWDB will fail and operations will terminate.

**Recommended actions:**

1. Check the application server log file for errors. The log messages are recorded in the Cisco_Home\eService\logs\eg_log_ApplicationServer_Name_ApplicationServer.log file when this issue occurs. Notice the host names in the logs (host AWDB machine). There will be one stack trace for the primary and another for the secondary AWDB when the application tries to rollover from primary to secondary connection pools and fails. Log messages indicating the rollover from the primary to the secondary database are also displayed.

   The log message appears as:
   'com.egain.platform.framework.dataaccess.exception.NoConnectionAvailableException: No connection available in pool IPCC_MSSQL_POOL_1'

   If the Listener service server connection pool to Unified CCE AWDB is exhausted, the same logs are seen in the Cisco_Home\eService\logs\eg_log_Services_Server_Name_ListenerServer.log file.

2. Increase the number of maximum connections configured for the AWDB in the application. The maximum number of connections is defined by the MaxCapacity setting in the System Console.

   a. Log into the system partition and go to the System Console.
   
   b. Open the Partitions folder in the Tree pane and select the default folder.
   
   c. In the Properties pane, navigate to the Databases tab and access the ipcc_db_prim (Primary AW Database) or ipcc_db_sec (Secondary AW Database) section.
d. Configure the MaxCapacity setting. Increase the value of the MaxCapacity setting for primary AWDB or secondary AWDB, if one is installed. For guidelines on the value that should be set, see the Cisco Unified Web and E-Mail Interaction Manager Solution Reference Network Design Guide.

Symptom 4: Agents Unable to Login

Agents are not able to log in to the Unified EIM and WIM application.

Cause 1: Services Required for Successful Login Not Running

To allow an integrated agent to successfully log in, the following services need to be up and running:

- CTIOS CTIOS1, CG1A, PG1A, PG2A in Unified CCE
- Listener service in Unified EIM & WIM should be connected to CTI Server

If these services are not running or are not configured properly, agents will not be able to log in.

Recommended actions:

1. From the ICM Service Control window, check if the following services are running:
   - Cisco ICM CG1A
   - Cisco ICM PG1A
Cisco ICM PG2A

If they are not running, start them.

Check the status of the services

2. From the Unified EIM and WIM System Console, check if the Listener service process and instances are running. Their state should be Running. If they are not running, start them. Make sure that the correct listener instance is running (Agent PG).

3. After fixing these issues, try to log in again.
Cause 2: Agent Not Associated With Any MRD

When an agent is not associated with any MRD, Unified CCE does not acknowledge the MEDIA_LOGIN_REQ message correctly. As a result, a failure message FAILURE_RESP is sent to Unified EIM and WIM and the agent is not logged in for that MRD.

Recommended actions:

1. From the System Console, set the logging level for the Listener process to INFO level. This level is required to view messages the Listener service sends to ARM.

2. After changing the log levels, check the Cisco_Home\eService\logs\eg_log_Service_Server_Name_Listener-process.log file. Verify that the MEDIA_LOGIN_REQ message is sent for all configured MRDs to Unified CCE. In the log file check if the MEDIA_LOGIN_REQ message returns a failure response during the agent login.

3. From the Unified CCE Configuration Manager, check if the MRD is configured properly, the agent is mapped to the correct MRD, and the MRD is configured properly in the Application path. For details on configuring these objects, see the Cisco Unified Web and E-Mail Interaction Manager Deployment and Maintenance Guide.

Logout Issues

Overview

When a mapped agent logs out of the Unified EIM and WIM Agent Console, the agent should also be logged out of Unified CCE for all MRDs. If there is a failure in this process, activities may be assigned to agents who are not logged in to Unified EIM and WIM.

Symptom: Activities Routed to Logged Out Agents

Activities are getting routed to agents who are not logged in to the Unified EIM and WIM Agent Console.

Cause 1: Agent Logout Status Not Updated in Unified CCE

When the agent’s session ends because the agent logs out of the Agent Console, or because of a permanent session timeout, the agent is logged out of Unified EIM and WIM, but a message to log out the agent is not sent to Unified CCE. As a result, Unified CCE keeps picking those agents for activity assignment, but the agents are not assigned activities in Unified EIM and WIM. This can cause a task count mismatch for agents between Unified EIM and WIM and Unified CCE.

An agent’s session is permanently timed out when the agent is inactive for the time defined, in seconds, in the partition level setting Deletion Time Out. For details about the setting, see Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Administration Console.
**Recommended actions:**

1. From the System Console, set the logging level for the Listener process to INFO level. This level is required to view messages the Listener service sends to ARM.

2. After changing the log levels, check the `Cisco_Home\eService\logs\eg_log_Services_Server_Name_Listener-process.log` file on the services server. Verify that the `MEDIA_LOGOUT_IND` message is sent for all configured MRDs to Unified CCE. After the agent’s session times out permanently, verify that the `MEDIA_LOGOUT_IND` message is going to Unified CCE to terminate the agent’s session.

**Cause 2: Synchronization of Agent Login State Fails**

Synchronization of agent login state between Unified CCE and Unified EIM and WIM goes out of sync when the `MEDIA_LOGOUT_IND` event is not reported to Unified CCE when the agent logs out from Unified EIM and WIM. Reporting fails because the agent is still shown as logged in within Unified CCE, but in Unified EIM and WIM, the agent has logged out. Agent logout from Unified EIM and WIM should trigger a `MEDIA_LOGOUT_IND` for logging out the agent from Unified CCE. Failure in sending the logout message to Unified CCE results in an incorrect agent state, and subsequent activity assignment to agent from Unified CCE continues.

**Recommended actions:**

1. From the System Console, set the logging level for the Listener-process to INFO level. This level is required to view messages the Listener service sends to ARM.

2. After changing the log levels, check the `Cisco_Home\eService\logs\eg_log_Services_Server_Name_Listener-process.log` file on the services server. Verify that the `MEDIA_LOGOUT_IND` message is sent for all configured MRDs to Unified CCE.

3. Check for any log message logged at the ERROR level. If there are any log messages logged at the ERROR level, capture all the Listener process logs and send the log files to Cisco TAC.

**User Interface Issues**

**Symptom 1: Blank Consoles Displayed**

Unified EIM and WIM console loads and appears as Done in the status bar, but the panes do not load despite resizing the window. Unified EIM and WIM application consoles load but display white screens.

**Recommended actions:**

1. Close the browser instance.

2. Clear the browser cache, and log in to the application.
Further analysis:

If the issue persists after logging in again, then collect data using the following tools and send the information to Cisco TAC.

1. For users trying to replicate the issue, enable Request Response Data and UI logging from the Utilities section of the Tools Console. For details about this tool, see “Request Response Data and UI Logging Utility” on page 38

2. Capture the HttpWatch or Fiddler traces by performing the actions that lead to the white screen with hourglass on the console. For details about these tools, see “Fiddler or HttpWatch” on page 40.
   a. Check for aborted 4XX or 5XX requests for JSP or JS.
   b. Check for any network connection errors.
c. Check the total time taken by JSP requests to fetch data from server.

Output from HttpWatch

Output from Fiddler
Symptom 2: Hourglass Appears When Performing Certain Console Actions

An hourglass appears while performing certain actions in the consoles.

Certain actions like clicking the **Refresh** button, using the spelling checker, clicking the **Pull, Transfer, Send, Send and Complete** buttons, etc. can lead to the UI freezing. Sometimes these actions may take longer than usual.

**Cause 1: Agent Desktop Not Configured Properly**

The agent’s desktop is not configured according to the *Cisco Unified Web and E-Mail Interaction Manager System Requirements* and the *Cisco Unified Web and E-Mail Interaction Manager Browser Settings Guide*.

**Recommended actions:**

- Follow these guides and validate that the agent’s desktop has the correct Internet Explorer version and that all the browser settings have been configured properly. If not, correct these and check if the issue is fixed after making these changes.

**Cause 2: Internet Explorer Browser Hangs**

When certain actions are performed by the user, the Internet Explorer browser hangs or freezes and the application does not recover from the freeze. The Internet Explorer browser process itself is hung and the application becomes unresponsive.

**Recommended actions:**

1. Try to launch the UI debugger and choose the option **Set default cursor > Run**. This changes the cursor from the hour glass (which prevents any user clicks) to the default cursor. Try performing some actions in the console. This step helps establish if the browser instance itself is unresponsive or the Unified EIM and WIM console is unresponsive and can be recovered by setting the cursor to default.
2. If the UI debugger cannot be launched, close all the Internet Explorer browser instances, clear the browser cache, and log in to the application again.

**Cause 3: Other Applications on User Desktop Using High CPU**

Other applications running on the agent’s desktop have high CPU usage. Because of this, the Unified EIM and WIM application does not receive enough system resources and the agent experiences slowness or browser hangs.

**Recommended actions:**

1. Start the Task Manager and check if the CPU usage for applications other than the Unified EIM and WIM is higher than 75%.
2. Stop the application that is consuming high CPU and see if this resolves the issue.
**Cause 4: Other Applications on User Desktop Using High Memory**

Other applications running on the agent’s desktop are consuming the majority of available memory.

**Recommended actions:**

1. Start the Task Manager and from the Performance tab, check if the available memory is less than 2 GB.

```
Check the available memory
```

2. Stop some of the applications running on the desktop and free up 2 GB of memory.

**Cause 5: Application Using High CPU and Memory on User Desktop**

The Unified EIM and WIM application running on the user desktop has high CPU and memory usage.

**Recommended actions:**

1. Start the Task Manager and check if the CPU usage of Unified EIM and WIM is higher than 75%. Check if the Memory usage of the Unified EIM and WIM IE process is more than 2 GB.
2. Refresh the Unified EIM and WIM console by clicking the **Refresh** button in the Console toolbar and see if the memory and CPU usage reduces.
3. Close all the Internet Explorer browser instances, clear the browser cache, clear the Java JAR cache from Control Panel > Java > General > Temporary Internet Files > Settings > Delete Files and log in to the application again.

**Further actions:**

Collect the following information and send the information to Cisco TAC.

1. Capture the HttpWatch or Fiddler traces by performing the actions that lead to the hourglass on the console.
2. Capture the following screen shots of the Windows task manager:
3. Capture the Internet Explorer version and system configuration information from My Computer > Properties > General.

**Cause 6: Issues on Server Side**

If the slowness is not confined to a particular agent desktop, but is observed by all the users working on the application, there could be a server side issue that is causing the slowness.

**Recommended actions:**

1. Ensure that for the given load, the hardware meets the requirements described in the Cisco Unified Web and E-Mail Interaction Manager Solutions Reference Network Design Guide.

2. On the application server from where the user is logged in, validate if any processes other than the Unified EIM and WIM java process are taking up the memory or CPU. Stop such applications and see if it resolves the problem. As a general guideline, on the server, java processes should not be consuming more than 1.6 GB of virtual memory space.

If the deployment uses a load balancer, you can find the application server on which the user is logged in by using the following query. The query provides the name of the application server used by the user in the server_name column.

```sql
select b.user_id, u.user_name, a.license_id, a.product_name, a.module_name, a.license_policy, s.server_name, c.* from egpl_license_user_consumption c
INNER JOIN egpl_license_user_assignment b
on b.pkey = c.userlicense_key
INNER JOIN egpl_license a
on a.pkey = b.license_key
INNER JOIN egpl_user u
on b.user_id = u.user_id AND u.user_name = User_Name
LEFT OUTER JOIN egpl_server_status s
on c.server_key = s.pkey

Where User_Name is the user’s login username.
```

**Cause 7: Database Issue**

If the slowness is not confined to a particular agent and if the issue is not on the application server, then there is a possibility that the issue is in the database.

**Recommended actions:**

1. Note if the application is generally slow or if there are any actions in the user interface that cause slowness.

2. Refer to the database troubleshooting guidelines for debugging this further. Look for DB queries that are taking a long time and if there are deadlocks on the database. See Database Issues on page 161.
Further Actions

If none of the recommended actions solve your problem, collect data using the following tools and send the information to Cisco TAC.

For details on running these tools, see “Troubleshooting Tools” on page 20.

1. For Users trying to replicate the issue, enable Request Response Data and UI logging from the Utilities section of the Tools Console. For details about this tool, see “Request Response Data and UI Logging Utility” on page 38

2. Run the following tools and access the application again. If there are specific actions that are causing the browser to freeze, repeat the actions to recreate the problem and capture the information using these tools.
   o HttpWatch or Fiddler traces
   o UI debugger logs

3. Also, send the log files: eg_log_server_Name_ApplicationServer.log and egpl_root_server_Name.log

4. If the hang is associated with a particular activity or user login, collect the audit trail for that activity or user from the database by running the following queries.
   
   ```
   select cast(dateadd(ss,event_date/1000,'1/1/1970')as datetime),* from egpl_event_history_case_mgmt where activity_id = Activity_ID order by event_date
   ```

   ```
   select cast(dateadd(ss,event_date/1000,'1/1/1970')as datetime),* from egpl_event_history_user where user_id = User_ID order by event_date
   ```

5. Details of the tasks the user was performing in the console when the issue was observed.

6. If the issue is related to the application server or database, collect the thread dump and the CPU usage of the JBoss application server where the slowness is being observed.
Unified CCE Configuration Issues

- Overview
- Configuration Issues
Overview

Accurate Unified CCE and Unified EIM and WIM configurations are critical to the successful startup of integration services (i.e., Listener & EAAS), activity assignments, and task management. This section covers various failure scenarios that may arise due to missing or incorrect Unified CCE or Unified EIM and WIM configurations.

Configuration Issues

Symptom 1: Listener Instance Stuck in “Connecting” State

While starting the Listener instance from the System Console, it is observed that the service stays in “Connecting” status and the state does not change to “Running”.

Cause: Incorrect Application Path in Unified CCE for the Peripheral Gateway

Application Path configuration is done through the Unified CCE Configuration Manager for the Peripheral Gateway (PG) that the Listener instance uses to connect to the CTI server. The Listener instance is configured in the Unified EIM and WIM System Console and mapped to the intended PG. If the Application Path members for the Application Path configuration are modified after deployment, as when they are configured for an incorrect PG in Unified CCE (one that is not used in the Unified EIM and WIM Listener instance configuration), the Listener instance will not be able to connect to the CTI server. As a result, the Listener instance’s state in the user interface will be stuck in a connecting state. When successfully connected to the CTI server, the correct state for Listener instance is Running.

If the Application Path configuration in Unified CCE is incorrect or missing, the OPEN_REQ request sent from the Listener instance to the CTI server will be rejected with a FAILURE_CONF by the CTI server.

Sample error message

![Sample error message](image_url)
Recommended actions:

1. Verify that the Application Path in Unified CCE is configured with the correct PG and has the right Application Path Members used for activity routing. Note that an Application Path Member is a Peripheral–MRD pair, and all combinations of Peripheral–MRD for the given PG must exist as Application Path Members for the given Application Path.

2. Ensure that the Listener instance in the System Console is configured to use the correct Agent PG for which the Application Path is configured in Unified CCE. When configured correctly with the correct Agent PG, the Listener instance state will transition to Running.

Symptom 2: MR PIM Stuck on “Attempting to Connect to MR Application…”

The following repetitive message is displayed in the MR PIM console: Attempting to connect to MR application...

Cause: MR PIM Port Does Not Match EAAS Instance Port

An incorrect MR PIM configuration in Unified CCE or for the EAAS Instance can lead to connectivity issues between the MR PIM and EAAS, resulting in the following repetitive message in the MR PIM console: Attempting to connect to MR application...

Sample error message in the MR PIM Console
In Unified EIM and WIM, the **MR Connection Port** for the EAAS instance is provided in the System Console at the partition level.

**MR Connection Port**

This is the port at which the EAAS server socket starts and the MR PIM will attempt to connect to the EAAS. In Unified CCE, the port number for MR PIM connection is provided by running/editing the Unified CCE setup configuration for MR PG.

**MR PIM Configuration**
**Recommended actions:**

1. From the System Console, ensure that the EAAS service process and instance are running. Start them if required.

2. Ensure that the Hostname or IP address provided in the MR PIM console is the same server where the EAAS service is hosted, that is, the Cisco Unified EIM & WIM services server.

3. Ensure that the MR PIM port number is the same as the port number configured for the EAAS instance.

4. Ensure that the port is free and available to use by MR PIM and EAAS.

5. Verify (from the MR logs) that an **OPEN_REQ** is sent from MR PIM to the EAAS, and that EAAS responded with **OPEN_CONF**. This ensures that the connectivity and communication are OK.
7

Retriever Issues

- Overview
- Email Retrieval Issues
- Email Parsing Issues
Overview

The Retriever service is a mail client that fetches incoming emails into the application from POP3 or IMAP mail servers. A set number of emails, defined in the partition level setting Number of Emails to Retrieve, are fetched for each alias at a time. The default number is 10. Once emails are fetched into the application, an email activity is created in the database for each incoming email. Problems that the Retriever might encounter are described in this chapter.

For more information about the Retriever service, see the Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to System Console.

Email Retrieval Issues

Symptom 1: Agents Not Receiving Email

Emails are not being retrieved. This can occur for one of the following reasons:

Cause 1: Alias Not Added to Retriever Instance

The alias has not been added to a retriever instance. This will affect all agents who work on emails sent to the alias, as new emails will not be fetched from the mailbox for that particular alias. No emails from that alias will be seen in the system. If the email retrieval issue is sporadic, or if some agents have received emails sent to this alias, this is not the likely cause of the issue.

Recommended actions:

- From the System Console, check if the alias has been added to a retriever instance.

Whenever a new alias is created in a department from the Administration Console, the alias must be added to the retriever instance and the retriever instance must be restarted.

Cause 2: Retriever Service Not Running

The Retriever service process and instance are not running. This will affect all email agents as no new emails are fetched into the system.

Recommended actions:

- From the System Console, ensure that retriever processes and instances are running.
Cause 3: Alias Not Configured Properly

The alias is not configured properly or there is some problem with the alias. This will affect all email agents as no new emails are fetched into the system.

Recommended actions:

1. Check the retriever log file for errors. The following log messages are recorded in the Cisco_Home\eService\logs\eg_log_Services_Server_Name rx-process.log file when this issue occurs.

   If POP3 or IMAP server information is not correct, the following exception is logged:
   
   javax.mail.MessagingException: Connect failed;
   java.net.UnknownHostException: <POP3_Server>

   If the username or password is incorrect, the following exception is logged:
   
   javax.mail.AuthenticationFailedException: Logon failure: unknown user name or bad password

2. From the Administration Console, check the following alias configuration:
   a. Check the server information provided for the POP3 or IMAP server.
   b. Check the usernames and passwords set for the alias.
   c. Ensure that the alias is active. Emails are not retrieved from inactive aliases.

3. To check the validity of the alias details, follow the listed steps.

   For POP3 servers:
   a. Telnet to the POP3 server using the following command (110 is the port number of the POP3 server):

      telnet Server_Name 110

   b. To check the login credentials, do the following:

      Type the following for the user name:
      User User Name

      Type the following for the password:
      Pass Password

      It should return OK if the login credentials are correct.

   For IMAP servers:
   a. Telnet to IMAP server using the following command (143 is the port number of the IMAP server):

      telnet Server_Name 143

   b. To check the login credentials, do the following:

      login User Name Password

      If the login credentials are correct, the message OK LOGIN Completed is returned.
Additional Information

Instance Monitors are very useful while debugging such problems through the user interface. It displays useful information including the aliases configured in the instance, their states (Active, Inactive, Login Failed, Disabled, or Connection Failed), the state of the instance, the start time, last run time, activities processed in the last run (in the last cycle), pending activities, and the throughput. From the System Console, configure and run monitors for the retriever instances. (See Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to System Console for steps to create a monitor). Using the monitors, check the following attributes.

- Check when the retriever was last run (the Last Run Time attribute will give you this time). If this is more than a few minutes prior to the current time, it indicates that the instance is not running as expected. This could be due to a problematic email, or because the retriever has network connection problems.

- For the aliases configured for the retriever, check the state of the alias. It can be one of the following.
  - **Active**: The alias is set as active and is working fine.
  - **Inactive**: The alias is set as inactive from the Administration Console.
  - **Login failed**: Authentication fails while connecting to the mailbox. This may be due to entering the wrong username or password while creating the alias.
  - **Disabled**: If there are consecutive authentication failures while connecting to the mailbox, the alias is disabled. In such a case, the service stops attempting to connect to the mail server using that alias.
  - **Connection failed**: Not able to connect to the mail server. This can happen because of a number of reasons. Check the following:
    - Check the mail server hostname and IP address configured for the alias. The hostname may have been changed after the alias was configured, and the alias configuration may need to be updated from the Administration Console.
    - Check if the mail server is functioning normally.
    - If the mail server is up, then check if the POP3 or IMAP services are running on the mail server.

Cause 4: Certificate Not Installed Properly for SSL Enabled Alias

The email account configured as alias is SSL enabled, but the certificate is not installed on the services server or it has expired. When this issue occurs, the following log message is recorded in the Cisco_Home\eService\logs\eg_log_Services_Server_Name_rx-process.log file.

```
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
```

Recommended actions:

1. Configure the SSL certificate on the services server.
2. From the Administration Console, check the alias properties to ensure that the **Use SSL** property is set to **Yes** and the correct port number is configured.

For detailed instructions on doing these tasks, see the Cisco Unified Web and E-mail Interaction Manager Installation Guide.
Cause 5: Non-SSL Account Configured as SSL

Email account on a non-SSL enabled POP3 or IMAP server is configured as SSL from the Administration Console. When this issue occurs, the following log message is recorded in the `Citco_Home\eService\logs\eg_log_services_server_Name_rx-process.log` file.

```
javax.net.ssl.SSLException: Unrecognized SSL message, plaintext connection?
```

**Recommended actions:**

- From the Administration Console, check the alias configuration. The property `Use SSL` in the Servers tab should be set to `No`.

For detailed instructions on doing these tasks, see the *Cisco Unified Web and E-mail Interaction Manager Administrator’s Guide to Email Resources*.

Cause 6: Retriever Service Hangs

The Retriever service may hang if it does not receive a response from the mail server.

**Recommended actions:**

1. Run the following query on the master database to get the `instance_id` for the retriever instance:

   ```sql
   select instance_id from egpl_dsm_instance where instance_name like 'RxInstanceName'
   
   where `RxInstanceName` is the name of the system’s retriever instance.
   ```

2. Check the retriever log file for errors. The following log message is recorded in the `Citco_Home\eService\logs\eg_log_services_server_Name_rx-process.log` file when this issue occurs.

   ```
   Rx Instance <instance_id> status is FALSE
   ```

3. Make sure that the value of the `Socket timeout for retriever` setting is not more than 15 minutes (default retriever failover delay). The `Socket timeout for retriever` setting is available in the Administration Console at the Partition level. The default value of the setting is 300 seconds.

4. From the System Console, restart the retriever service process and instance.
Symptom 2: Administrator Gets “Large Email has Been Received” Notification

The following email notification is received by the email address defined in the partition setting To: address for notifications from services:

Subject: Retriever - large email has been received!

Content: Email was too large. It has not been retrieved from the mail server (it has been skipped).

Email details:
Addressed to: Original email TO addresses
Sent by: Original email FROM address
Email subject: Original email subject

Cause: Email Size is Larger Than 'Maximum Email Size' Setting

The retriever has the ability to skip or delete emails that are large in size, or have large attachments. The exact size is specified in the setting Maximum email size for Retriever. Such emails are either skipped or deleted from the POP3 server based on the action defined by the preference setting Action for large email.

Recommended actions:
1. Telnet to the mail server and check the size of the email by using the list command.
2. If you wish to retrieve the large email, go to the Administration Console and increase the value of the partition level setting Maximum email size for Retriever to greater than the size of the email.
3. Restart the retriever process and instance from the System Console.

Symptom 3: Attachments Missing From Emails

Attachments are missing from the incoming emails. Either the attachments do not show with the email, or they show as blocked attachments.

Cause: Particular File Extensions are Blocked

This can occur when particular file extensions are blocked for a department, and the department level settings are configured to delete such attachments or quarantine them.

Recommended actions:
1. In the Administration Console, in the Tree pane, browse to Department_Name > Email > Blocked File Extensions. Check the list of blocked file extensions.
2. Check the department level setting **Action on blocked attachments**. If the value of the setting is **Delete**, then all the blocked attachments are deleted. If the value of the setting is **Quarantine**, then the attachments get saved at a different location and can be restored or deleted. In the Tree pane, browse to **Department_Name** > **Email** > **Blocked File Extensions**. From the List pane toolbar, click the **Blocked attachments** button, to see a list of activity IDs and files names of the blocked attachments. If required, restore the blocked attachments, or delete them.

**Symptom 4: Emails Retrieved Very Slowly**

Emails are getting retrieved, but a delay is observed in the retriever process.

**Cause 1: Database Slowness**

Emails are retrieved very slowly possible because of database slowness. If database queries take more than 10 seconds to execute, they are logged into the `Cisco_Home\eservice\logs\eg_log_dal_connpool_services_server_rx-process.log` file. Such entries indicate database slowness.

**Recommended actions:**

- Refer to the Database troubleshooting guidelines to debug this further. See “Database Issues” on page 161.

**Cause 2: Services Server and POP3 Servers are on Different Networks**

Services server and POP3 server are on different networks or in different geographies. The downloading of email content and attachments takes time in such cases, causing overall slowness.

**Recommended actions:**

1. Run the following commands to check if there are connection issues:

   For POP3 servers:
   a. Telnet to POP3 server using the following command (110 is the port number of the POP3 server):
      
      `telnet Server_Name 110`
   b. To login, do the following:
      
      Type the following for the user name:
      
      `User User Name`
   c. Type the following for the password:
      
      `Pass Password`
   d. Run the following commands and see if the response is returned instantly. If not, it indicates the connection between the services server and POP3 server is slow.
      
      To get status of number of messages:
      
      `STAT`
      
      To list messages along with their size:
For IMAP servers, do the following:

a. Telnet to IMAP server using the following command (143 is the port number of the IMAP server):
   
   `telnet Server_Name 143`

b. To login, do the following:
   
   `login User_Name Password`

c. Run the following commands and see if the response is returned instantly. If not, it indicates the connection between the services server and IMAP server is slow.

   `SELECT INBOX`  
   `FETCH 1 full`

The recommendation is to keep the services server and POP3 server in the same network and geography.

Symptom 5: Administrator Gets Retriever - Skipping Email Retrieval Notification

The following email notification is received by the email address defined in the partition setting **To: address for notifications from services:**

**Subject:**
Retriever - Skipping email retrieval!

**Content:**
Skipped Email, as it has already been retrieved or there was a problem with retrieval.

**Email details:**

- **Addressed to:** Original email To addresses
- **Sent by:** Original email From address
- **Email subject:** Original email subject

**Cause 1: Email is Retrieved but Not Deleted in Previous Cycle**

When an email is retrieved, the retriever deletes it from the POP3/IMAP server. But if that deletion fails - e.g. network problems - then, in the next cycle, the retriever encounters the same email. The retriever then considers such emails as duplicate, sends this notification, and skips it. Another potential reason behind these notifications is that the email itself came multiple times to the alias inbox. If the message-ID header of the email matches with emails already retrieved, then the email is considered a duplicate.

**Recommended actions:**

- Delete the emails from the alias inbox using another client.
**Cause 2: Duplicate Email is Received**

Please refer to Cause 1: Email is Retrieved but Not Deleted in Previous Cycle on page 84

**Recommended actions:**

- Delete the emails from the alias inbox using another client.

---

**Email Parsing Issues**

**Symptom 1: “Email Reading Failure” Notification Sent to Administrators**

When there are parsing failures while retrieving emails, a notification Retriever - Email Reading Failure is sent to the email address configured in the partition level setting To: Address for Notifications From Services.

**Cause: Retriever Unable to Parse Emails**

This can occur for one of the following reasons:

- Messages are not according to RFC 822 message standards. For example, Content type field is missing from the message header.
- Message ID is missing.
- There is no start boundary.
- The mail header character set value is not recognized by Java Mail. For example, it contains characters like iso 8859-1 whereas the correct format is iso-8859-1.

When the retriever is unable to parse emails, emails are inserted in raw format in the Cisco_Home\eService\storage\Partition_ID\mail\Exception Emails\RxExcepEmails.txt file.

**Recommended actions:**

1. Check the retriever log file for errors. The following log message is recorded in the Cisco_Home\eService\logs\eg_log_Services_Server_Name_rx-process.log file when this issue occurs.

   com.egain.mail.module.retriever.exception.FailedToParseEmailException

2. Collect the following files for the time when the parsing issues were faced and send the files to Cisco TAC for further analysis.

   - Cisco_Home\eService\logs\eg_log_Services_Server_Name_rx-process.log
   - Cisco_Home\eService\storage\1\mail\Exception Emails\RxExcepEmails.txt
Symptom 2: Emails are Displayed in Plain Text

Emails in rich text format are displayed in plain text. This happens for emails sent from Microsoft Outlook.

Cause: Retriever is Unable to Interpret File Format From MS Outlook

When the Rich Text format is used, Microsoft Outlook uses a proprietary format called TNEF (Transport Neutral Encapsulation Format) to create such emails. Such emails have two parts: a plain-text part that contains the content of the email, and an encoded attachment (generally named Winmail.dat) which contains the formatting information. The retriever is only able to store the plain-text part of the email.

Recommended actions:

There is a workaround for this in the Microsoft Exchange Server.

- From the Protocol > POP3/IMAP > Message Format tab, enable the setting Provide message body as HTML.

If this setting is enabled, the exchange server itself converts the Rich Text content of incoming emails into HTML, which the retriever is able to parse and save. This setting can either be configured as the default, applied to all aliases, or for each alias separately. This is specific to MS Exchange servers, and other mail servers may not have such a facility.
Dispatcher Issues

- Overview
- Setup and Performance Issues
- Email Dispatch Issues
Overview

The Dispatcher is a service that interacts with an SMTP or ESMTP server to send emails. This chapter discusses problems that the Dispatcher may encounter while trying to send outgoing emails.

To learn more about the Dispatcher service, see the Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to System Console.

Setup and Performance Issues

Symptom 1: Dispatcher Service Hangs or Crashes

The Dispatcher service crashes or hangs, preventing emails from being sent out of the system.

Cause: The System has Insufficient Memory

The Dispatcher service can hang if the system has insufficient memory.

Recommended actions:

1. Check the dispatcher log file for errors. The following log message is recorded in the \Cisco_Home\eService\logs\eg_log_services_Server_Name_dx-process.log file when this issue occurs.

   Instance Failed. Exiting.. == > <dx_instance_id>, java.lang.OutOfMemoryError

2. If emails with large content are sent out from the system, adjust the value of the partition level settings Number of new emails to dispatch and Number of retry emails to dispatch so that less number of emails are picked by the dispatcher. Use the following query to get the size of email contents of the top 100 (default batch size of new activities) activities. This size doesn't include attachment sizes. Dispatcher also loads actual attachment content in memory only while sending email. If the total size of the email is 60-70 MB, contents of emails can be considered as large.

   SELECT sum(email.email_size) total_bytes
   FROM (SELECT top 100 a.activity_id, e.email_size
   FROM egpl_casemgmt_activity a, egml_email e
   WHERE a.activity_id = e.activity_id
   AND a.activity_status = 7000) email

3. From the System Console, restart the Dispatcher service processes and instances.
Symptom 2: Unable to Connect to SMTP or ESMTP Server
Dispatcher service is not able to connect to the SMTP or ESMTP server.

Cause 1: SMTP or ESMTP Server Unavailable
If the SMTP or ESMTP server is unavailable, all emails that use this server are not dispatched.

Recommended actions:
1. Check the dispatcher log file for errors. The following log message is recorded in the
   Cisco_Home\eservice\logs\eg_log_Services_Server_Name_dx-process.log file when this issue
   occurs.
   java.net.SocketTimeoutException: Read timed out
2. Start the SMTP or ESMTP server.
3. Start the SMTP service.

Cause 2: Connections to SMTP or ESMTP Server Exceed Maximum Number
Connections to the SMTP or ESMTP server have exceeded the maximum number of connections allowed for
that server. Emails will not be sent out if the SMTP server does not allow the establishment of a connection.
Typical errors that are seen are:
- Mail Enable: 451 ESMTP MailEnable Service temporarily refused connection at
  04/26/11 12:24:29 from IP (10.10.51.231) because the server is too busy.
- MS Exchange: 421 4.7.1 - Connection Refused -- Too many connections

Recommended actions:
1. Contact your IT administrator to increase the number of connections. If your connection limit is IP based,
   increase the number of connections for the application server and services server.
2. Close any unnecessary mail clients connecting to the SMTP server.

Cause 3: Connection Times Out
Intermittently, due to network problems, the connection times out while connecting to the SMTP or ESMTP
server.

Recommended actions:
1. Check the dispatcher log file for errors. The following log message is recorded in the
   Cisco_Home\eservice\logs\eg_log_Services_Server_Name_dx-process.log file when this issue
   occurs.
   java.net.ConnectException: Connection refused:
If this exception is observed frequently, you can change the value of the DX.SocketTimeout setting. If you
do not want to increase this value, the Dispatcher will again try to connect and send emails in the next cycle
after 30 seconds.
2. The `DX.SocketTimeout` setting is available in the `EGPL_CONFIG_PROPERTY` table in the active database. The default value is 5 minutes. You can increase it up to 10 minutes.

Run the following query on the active database to find the current value of the setting:

```
SELECT * from EGPL_CONFIG_PROPERTY where name = 'DX.SocketTimeout' and DOMAIN = 'dispatcher.egpl_dispatcherconfig.properties'
```

Run the following query on the active database to update this setting:

```
UPDATE EGPL_CONFIG_PROPERTY SET VALUE = 'New_Value' WHERE name = 'DX.SocketTimeout' and DOMAIN = 'dispatcher.egpl_dispatcherconfig.properties'
```

3. Restart the Dispatcher Service process and instance after changing the setting.

---

### Email Dispatch Issues

#### Symptom 1: Emails Not Dispatched

Emails are not dispatched. If the system is configured to notify administrators when the activities that are not dispatched reaches a certain number, an email notification is sent by the system.

#### Cause 1: Incorrect SMTP or ESMTP Information

While configuring the alias in Unified EIM & WIM, incorrect server information is provided for the ESMTP or SMTP server. If this information is incorrect, all emails that use this server are not dispatched.

**Recommended actions:**

1. Check the dispatcher log file for errors. The following log messages are recorded in the `Cisco_Home\eService\logs\eg_Log_Services_Server_Name_dx-process.log` file when this issue occurs.
   - For SMTP server: `javax.mail.MessagingException: Unknown SMTP host x.x.x.x`
   - For ESMTP server: `javax.mail.AuthenticationFailedException` (indicating username and password information is incorrect)

2. From the Administration Console, check the alias configuration. Check the protocol used, the name or IP address of the server, the username, and password (for ESMTP server).
Cause 2: Port 25 Blocked on Services Server

The virus scanner or the firewall on the services server is blocking port 25. No outgoing emails are sent out if port 25 (default SMTP post) is blocked.

Recommended actions:

1. Check the dispatcher log file for errors. The following log message is recorded in the Cisco_Home\eService\logs\eg_log_Services_Server_Name_dx-process.log file when this issue occurs.
   
   javax.mail.MessagingException: Could not connect to SMTP host: x.x.x.x, port: 25;

2. Check the firewall or the virus scanner on the services server to ensure that port 25 is not blocked.

Cause 3: Services Server IP Address Blocked on SMTP Server

The email relay for the services server IP address is blocked on the SMTP server.

Recommended actions:

1. Check the dispatcher log file for errors. The following log message is recorded in the Cisco_Home\eService\logs\eg_log_Services_Server_Name_dx-process.log file when this issue occurs.
   
   javax.mail.MessagingException: Could not connect to SMTP host: x.x.x.x, port: 25, response: -1

   The response: -1 differentiates this condition from the previous one.

2. If you find this exception, contact your mail server administrator to unblock the services server IP address for sending emails.

Cause 4: Emails Considered as Spam by SMTP Server

Emails are refused by the SMTP server because they are considered spam emails, or they have attachments that are restricted by the server. If a particular email address or particular subject is configured as spam on the SMTP server, emails using this address or subject are not dispatched.

Recommended actions:

1. Check the dispatcher log file for errors. The following log message is recorded in the Cisco_Home\eService\logs\eg_log_Services_Server_Name_dx-process.log file when this issue occurs.
   
   554 Message refused

2. If you find this exception, contact your IT administrator to remove the email address or subject from the spam list.
Cause 5: Attachments Considered as Malicious by SMTP Server

Emails contain attachments perceived as malicious by the SMTP server. Emails with “malicious” attachments are not sent out.

Recommended actions:

1. Check the dispatcher log file for errors. The following log messages are recorded in the
Cisco_Home\eService\logs\eg_log_Services_Server_Name_dx-process.log file when this issue occurs.
   - 550-Restricted file-type in attachment
   - 550-Potentially executable content. If you meant to send this file then please package it up as a zip file and resend it

Such emails are marked as permanently undispatchable.

2. If the attachments are valid, then contact your mail server administrator to remove such file extensions from the blocked file list. This will ensure that such attachments are not restricted in future. The earlier activity cannot be resubmitted for processing.

Cause 6: Email Size Exceeds Maximum Allowed Size

The server keeps rejecting emails higher than the allowed size. The allowed size is controlled by the partition level setting Maximum body size for dispatcher. Outgoing emails that are larger (content+attachments) than the maximum size allowed on the SMTP server are not sent out.

Recommended actions:

1. Check the dispatcher log file for errors. The following log message is recorded in the Cisco_Home\eService\logs\eg_log_Services_Server_Name_dx-process.log file when this issue occurs.
   - 552 Message size exceeds maximum permitted

2. Contact your IT administrator to increase the size limit of emails.

Cause 7: “Read” Permission Not Granted on the Storage Directory

In this case, all emails with attachments will not be sent out.

Recommended actions:

1. Check the dispatcher log file for errors. The following log message is recorded in the Cisco_Home\eService\logs\eg_log_Services_Server_Name_dx-process.log file when this issue occurs.
   - java.io.FileNotFoundException: <attachment_file_name> (Access is denied)

2. On the file server, for the following folder, assign the read permission to the user account used to run the Unified EIM and WIM application: Cisco_Home\eService\storage\1\mail\attachments
Cause 8: Relaying Not Allowed for To Addresses of Emails

Emails are not sent out to email addresses to which relaying is not allowed.

Recommended actions:
1. Check the dispatcher log file for errors. The following log message is recorded in the Cisco_Home\eService\logs\eg_log_Services_Server_Name_dx-process.log file when this issue occurs.

   com.sun.mail.smtp.SMTPAddressFailedException: 550 5.7.1 Unable to relay for <TO_address>

2. If the email address is valid, ask your mail server administrator to allow relaying for problematic addresses.

Cause 9: Certificate Not Installed Properly for SSL Enabled Alias

The email account configured as alias is SSL enabled, but the certificate is not installed on the services server or it has expired. When this issue occurs, the following log message is recorded in the Cisco_Home\eService\logs\eg_log_Services_Server_Name_dx-process.log file.

   javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed:
   sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target

Recommended actions:
1. Configure the SSL certificate on the services server.
2. From the Administration Console, check the alias properties to ensure that the Use SSL property is set to Yes and the correct port number is configured.

   For detailed instructions on doing these tasks, see the Cisco Unified Web and E-Mail Interaction Manager Installation Guide.

Cause 10: Non-SSL Account Configured as SSL

Email account on a non-SSL enabled POP3 or IMAP server is configured as SSL from the Administration Console. When this issue occurs, the following log message is recorded in the Cisco_Home\eService\logs\eg_log_Services_Server_Name_dx-process.log file.

   javax.net.ssl.SSLException: Unrecognized SSL message, plaintext connection?

Recommended actions:
- From the Administration Console, check the alias configuration. The property Use SSL in the Servers tab should be set to No.

   For detailed instructions on doing these tasks, see the Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Email Resources.
Symptom 2: Agent Receives Attachment Size Error Message

Agents attempting to send emails with an attachment size greater than 25 MB receive an error message saying:

The attachment size exceeds the allowable limit of 25 MB for mail activities. Reduce the size or number of attachments and try again.

Cause: Email Attachment’s Size Larger Than Outgoing Email Size Limit

Administrators at the partition level can set an email attachment size limit on outgoing emails through the configuration setting Maximum email attachment size for dispatcher (MB). Outgoing emails with attachments that have a size greater than the specified amount will not be dispatched. This setting’s value is 25 MB by default.

Recommended Actions:

Do one of the following:

- Access partition level settings and increase Maximum email size for dispatcher (MB) to greater than 25 MB.
- Remove attachments or reduce contents of the email to a size less than the Maximum email size for dispatcher (MB) setting’s value.

Symptom 3: Agent Receives Email Content Size Error Message

Agents attempting to send emails with a body size greater than 100 KB receive an error message saying:

The email is too large. Reduce this email body size to less than 100 KB and send.

Cause: Email Body Size Larger Than Outgoing Email Size Limit

Administrators at the partition level can set an email body size limit on outgoing emails through the configuration setting Maximum body size for dispatcher (KB). Outgoing emails with a content size greater than the specified amount will not be dispatched. This setting’s value is 100 KB by default.

Recommended Actions:

Do one of the following:

- Access partition level settings and increase Maximum body size for dispatcher (KB) to greater than 100 KB.
- Reduce the contents of the email to less than the setting’s value and resend the email.

Symptom 4: Agent Receives Email Size Error Message

Agents attempting to send emails with a size greater than 25 MB receive an error message saying:

The email is too large. Reduce this email size to less than 25 MB and send.
Cause: Email Size Larger Than Outgoing Email Size Limit

Administrators at the partition level can set a total email size limit (email content and attachments) on outgoing emails through the configuration setting **Maximum email size for dispatcher (MB)**. Outgoing emails with a total size greater than the specified amount will not be dispatched. This setting’s value is 25 MB by default.

**Recommended Actions:**

Do one of the following:

- Access partition level settings and increase **Maximum email size for dispatcher (MB)** to greater than 25 MB.
- Reduce the contents of the email to less than the setting’s value and resend the email.
Integration Services Issues

- Overview
- Listener Service Issues
- External Agent Assignment Service Issues
Overview

This chapter describes the steps that should be followed to induce problems related to the External Agent Assignment Service (EAAS) and the Listener service.

This chapter only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

Listener Service Issues

Symptom 1: “Listener Instance Cannot be Started” Error Displayed

The following error occurs while starting the Listener service instance: 

```
Listener Instance cannot be started. There was a failure in creating Agent PG connection.
```

Cause 1: Primary Unified CCE AW Database Not Configured Correctly

If the deployment only has a primary Unified CCE Administration Workstation Database (AWDB), and the database is not running or not configured properly, this issue can occur.

For recommended actions for this problem, see “Cause 1: Primary Unified CCE AW Database Not Configured Correctly” on page 60. In Step One, use the log file `eg_log_Services_Server_Name_Listener-process.log` on the services server.

Cause 2: Secondary Unified CCE AW Database Not Configured Correctly

If the deployment has a primary and secondary Unified CCE Administration Workstation Database (AWDB), and the primary database server becomes unavailable, the application is unable to connect to the secondary database if the secondary database is not running or is not configured properly.

For recommended actions for this problem, see “Cause 2: Secondary Unified CCE AW Database Not Configured Correctly” on page 60. In Step One, use the log file `eg_log_Services_Server_Name_Listener-process.log` on the services server.

Symptom 2: Listener Instance Stuck in Connecting State

While starting the Listener service instance from the System Console, it is observed that the service stays in “Connecting to server” status and the state does not change to “Running”. As a result, agents are not able to log in to Unified EIM and WIM.

For causes and recommended actions, see “Symptom 1: Listener Instance Stuck in “Connecting” State” on page 73.
External Agent Assignment Service Issues

Symptom 1: Unable to Start External Agent Assignment Service Instance

The following error occurs while starting the External Agent Assignment Service (EAAS) instance:

Can not start EAAS instance at specified port. Please specify new port.

Cause: Port Configured for EAAS is Already in Use

The EAAS instance acts as a server to MR PIM clients. When the EAAS instance is started, it internally starts a socket server listening on a port specified through the MR Connection port settings configured through the EAAS instance properties from the System Console. If the specified port is not free at the services server, the EAAS instance startup will fail.

Recommended actions:

1. From the System Console, from the EAAS instance properties, note down the value of the MR Connection Port field.
2. Run the following command on the services server to verify that the MR Connection Port is free.
   ```
   netstat -an -p tcp
   ```
3. From the results of the command, check the list of the ports in the Local Address column. The ports should not match the MR Connection Port number.
4. If the port is in use, try using a different port in the EAAS instance and see if the service instance starts.

Symptom 2: EAAS “Did Not Start” Error While Starting Service Instance

The following error occurs while starting the External Agent Assignment Service (EAAS) instance:

EAAS Instance could not be started as Expanded Call Variables failed to get registered. Please verify Expanded Call Variables configuration and database connectivity between Unified EIM & WIM and UCCE Administration Workstation

Cause 1: Primary Unified CCE AW Database Not Configured Correctly

If the deployment only has a primary Unified CCE Administration Workstation Database (AWDB), and the database is not running or not configured properly, then this issue can occur.

For recommended actions for this problem, See “Cause 1: Primary Unified CCE AW Database Not Configured Correctly” on page 60. In Step One, use the log file `eg_log_Services_Server_Name_EAAS_process.log` on the services server.
Cause 2: Secondary Unified CCE AW Database Not Configured Correctly

If the deployment has a primary and secondary Unified CCE Administration Workstation Database (AWDB), and the primary database server becomes unavailable, the application is unable to connect to the secondary database if the secondary database is not running or is not configured properly.

For recommended actions for this problem, See “Cause 2: Secondary Unified CCE AW Database Not Configured Correctly” on page 60. In Step one, use the log file `eg_log_services_server_Name_EAAS-process.log` on the services server.
Email and Workflow Issues

- Overview
- Activity Routing Issues
Overview

When emails enter the system they are processed by workflows. They are routed to users, queues, or other departments based on the various rules configured in the workflow. This chapter describes the various workflow issues that occur when activities are routed to the exception queue instead of their destination queue or user.

By default, an exception queue is created in every department. Activities are routed to the exception queue when one of the following conditions is met:

- There are no active inbound workflows in the department.
- A workflow faces an error while processing activities.
- The queue used in a workflow is made inactive. All the activities coming to the inactive queue are routed to the exception queue.
- Emails are bounced back.
- A new_task_failure message is returned by Unified CCE.

To learn more about workflows and routing, see the Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Routing and Workflows.

Activity Routing Issues

A Note About Routing

In integrated systems, activities of type=1 and sub_type=1 are the only activities processed by EAAS and sent to Unified CCE. If the start workflow is modified to allow emails which meet exception conditions such as undeliverable emails, out of office replies etc., these will remain in the integrated queue, and are not sent to Unified CCE since the sub_type of these emails is not 1.

Symptom 1: Activities Routed to Exception Queue

Activities are not processed by workflows and are routed to the exception queue.

Cause 1: Inbound Workflow Does Not Exist

For a particular email alias, the inbound workflow is not configured correctly to route activities. It is also possible that the workflow does not exist.

Recommended actions:

1. From the Administration Console, browse to Department_name > Workflows, and check to make sure that a workflow is configured for routing activities.
2. Check all the workflows in the department to see if a workflow exists for the alias. You can verify this by looking at the Start node of Inbound workflows.
3. If the workflow exists, make sure it is Active. You can check this from the General tab of the workflow.
4. If the workflow does not exist, create one.

**Cause 2: End Node in Inbound Workflow is an Inactive Workflow**

When one workflow is configured to route activities to another workflow, the workflows are chained together. For routing to occur properly, all the workflows in the chain need to be active. If the terminating node in the inbound workflow is another workflow that is not active, activities are routed to the exception queue.

**Recommended actions:**

1. Check the `Cisco_Home\eservice\logs\eg_log\Services_Server_Name\rules-process.log` file for statements like "RulesEngine could not route to the chained workflow as the chained workflow is inactive: Workflow Name = active_inbound_workflow_name"
2. If the log statement exists, log in to the Administration Console and in the inbound workflow, check if the chained workflow is selected in the Add existing workflow node.
3. If the chained workflow is not displayed in the Add existing workflow node, it means that the workflow was made inactive. Access the workflow and make it active.

**Cause 3: Transfer Node in Inbound Workflow is an Inactive Workflow**

When the workflow is configured to route activities to a workflow in another department, the Start workflow – transfer workflow needs to be made active in the other department. If the workflow is made inactive, activities are routed to the exception queue.

**Recommended actions:**

1. Check the `Cisco_Home\eservice\logs\eg_log\Services_Server_Name\rules-process.log` file for statements like "Rules Engine could not Transfer this activity because there is no Active Transfer Workflow in that department: Workflow Name = active_inbound_workflow_name"
2. If the log statement exists, log in to the Administration Console and in the inbound workflow, check if the workflow from the other department is selected in the Add existing department node.
3. If the workflow is not displayed in the Add existing department node, it means that the workflow was made inactive. Go to the other department, access the Start workflow – transfer workflow and make it active.

**Cause 4: Inactive Queue in Inbound Workflow**

A queue to which the workflow is expected to route activities has been made inactive and as a result, activities are routed to the exception queue.

**Recommended actions:**

1. Check the `Cisco_Home\eservice\logs\eg_log\Services_Server_Name\rules-process.log` file for statements like "Routing Engine failed to route to Queue Queue_name as Queue is Inactive"
2. If the log statement exists, log in to the Administration Console and in the **Workflows > Queue** node, check if the queue used in the workflow is inactive.

3. Make the queue active and see if it solves the problem.

**Cause 5: Emails are Bounced Back**

When the retriever picks up an email, it checks it for delivery exception words and phrases configured in the system. If the email address or subject contains any of those words, the activity subtype is changed to **Email-permanent undeliverable** or **Email-temporary undeliverable**, based on the failure type configured for that word or phrase. The email activity is sent to the exception queue by the Standard Start Workflow.

**Recommended actions:**

1. Run the following query on the `egpl_casemgmt_activity` table:
   ```sql
   select activity_sub_type from egpl_casemgmt_activity where activity_id=activity_ID
   ```
   Check the value in the `activity_sub_type` column. If the value is 4 or 5, it means that the email is considered a bounced back email and it has been routed to the Exception Queue.

2. In the Administration Console, browse to **Department_Name > Email > Email Delivery Exception**. Check the list of email delivery exceptions to see if any of the words that are part of this list are present in the “Subject” or the “From email address” fields of the email.

3. If you do not want the phrase to be considered for delivery exceptions, delete it from the list.

**Cause 6: Database Queries for Workflow Taking Long Time**

When the Workflow Engine service processes an email, the database queries for the workflow run over the allocated time, and the execution of such queries is cancelled. As a result, the workflow is unable to finish processing activities and routes them to the exception queue.

The allocated time for the queries is defined in the `isValidQueryTimeOut` property available on the services server in the `Cisco_Home\eService\lib\configurations.zip\egpl_common_config.properties` file. The default value is 120 seconds.

**Recommended actions:**

1. Check the `Cisco_Home\eService\logs\eg_log_Services_Server_Name_rules-process.log` file for a log statement like “Deadlock inspector has cancelled the query”.

2. If such exceptions are observed, refer to the database troubleshooting guidelines. See “Database Issues” on page 161.

**Cause 7: NEW_TASK_FAILURES Message With Different Reason Codes**

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

When email activities are sent to Unified CCE by EAAS for routing, Unified EIM expects a `DO_THIS_WITH_TASK` message with an available agent’s ID for successfully routing the email activity to an agent. When Unified CCE does not send a `DO_THIS_WITH_TASK` message but sends a `NEW_TASK_FAILURE` message, emails are not routed to agents. Such emails get routed to the exception queue.
NEW_TASK from Unified EIM & WIM can fail due to issues in Unified CCE router configurations. The reasons for failure can be identified from the NEW_TASK_FAILURE message for the NEW_TASK in the MR PG logs.

**Recommended actions:**

1. Run the following query on the Cisco Unified EIM & WIM active database:

   ```
   SELECT * FROM egpl_casemgmt_activity WHERE activity_sub_status = 1 AND assigned_to = -1
   ```

   It will give a list of email activities that are not assigned to any agent.

2. From the MR PG logs available in Unified CCE, look for the Dialogue ID for the activities you identified in Step 1. The message will look like this:

   ```
   Message = NEW_TASK; Length = 84 bytes
   DialogueID = (3) Hex 00000003 (the dialogueID is displayed in this line)
   SendSeqNo = (1) Hex 00000001
   MRDomainID = (5010) Hex 00001392
   PreviousTask = -1:-1:-1
   PreferredAgent = Undefined
   Service = (0) Hex 00000000
   CiscoReserved = (0) Hex 00000000
   ScriptSelector: SS_Email_MR_D_Ravi
   ECC Variable Name: user.cim.activity.id Value: 1138 (the activity ID is displayed in this line)
   ```

3. In the same MR PG log file, search for the Dialogue ID you noted down in Step 2 and look for the NEW_TASK_FAILURE_EVENT message and the ReasonCode for the DialogueID. For example, the message will look like:

   ```
   Message = NEW_TASK_FAILURE_EVENT; Length = 12 bytes (the NEW_TASK_FAILURE_EVENT is displayed in this line)
   DialogueID = (3) Hex 00000003 (the dialogueID is displayed in this line)
   SendSeqNo = (1) Hex 00000001
   ReasonCode = (209) Hex 000000d1 (the ReasonCode is displayed in this line)
   ```

Some of the common NEW_TASK_FAILURE reason code are described here. For details of the Reason code, refer to the "Reason Code" section of the document: Cisco MR Interface Specification.

- Reason Code 205: ICM Times out before finding an agent. Verify the ICM scripts used for email routing for any unwanted wait nodes.
- Reason Code 206: Invalid dialed number or script selector.
- Reason Code 204: Invalid MRD ID. The MRD ID mentioned in the NEW_TASK message is not found in ICM.
- Reason Code 201: Invalid NEW_TASK message
- Reason Code 202: ICM Media routing has been disabled
- Reason Code 207: No target chosen by the router
Reason Code 208: Router released the call/task
Reason Code 209: Unknown routing problem
Reason Code 210: Duplicate new task request
Reason Code 211: Unsupported service requested

These reason codes will help you identify the problems in Unified CCE. Fix these problems and see if new incoming activities are routed to agents.

Further Analysis

If none of the above mentioned recommended actions solve your problem, then collect data using the following tools and send the information to Cisco TAC.

1. Cisco_Home\eService\logs\eg_log_Services_Server_Name_rules-process.log
2. Cisco_Home\eService\logs\eg_log_Services_Server_Name_rules-cache-process.log
3. Get details of the notes attached to the activity from the egpl_notes table.
   
   ```sql
   select * from egpl_notes where note_of_id = @Activity_ID
   ```
   
   Note: Value of the Note_of_ID column is the ID of the activity.
4. If possible, set the logging level of rules process to INFO. This level logging gives you information about the workflow executed on the activity as well as the sequence of nodes and rules executed on the activity.
5. Collect the Audit trail of the activity by doing one of the following:
   * Search for the activity from Search window of the Agent Console.
   * Run the following query on egpl_event_history_case_mgmt table.
     ```sql
     select cast(dateadd(ss,event_date/1000,'1-1-1970') as datetime) as EVENT_TIME, * from egpl_event_history_case_mgmt where activity_id = @Activity_ID order by event_date
     ```
     Note: Value of the Rule_ID column is the ID of the workflow applied on that activity.
6. Run the following queries and gather data using these queries:
   * Select * from egpl_case_mgmt_activity where activity_id = @Activity_ID
   * Select * from egml_email where activity_id = @Activity_ID
   * Select * from egml_email_data where email_id = (select email_id from egml_email where activity_id = @Activity_ID)
     ```sql
     select cast(dateadd(ss,event_date/1000,'1-1-1970') as datetime) as EVENT_TIME, * from egpl_event_history_case_mgmt where activity_id = @Activity_ID order by event_date
     ```
   * Select * from egml_email_address where email_id = (select email_id from egml_email where activity_id = @Activity_ID)
   * Select * from egml_email_attachment where email_id = (select email_id from egml_email where activity_id = @Activity_ID)
   * Select * from egpl_workflow_association where workflow_id = (select workflow_id from egpl_workflow where workflow_name = 'Workflow_Name')
Select * from egpl_workflow_association_ex where workflow_id = (select workflow_id from egpl_workflow where workflow_name = 'Workflow_Name')

Select * from egml_mailhost

7. For messaging server issues, provide all logs from the $Cisco_Home\eService\logs$ folder.
8. From Unified CCE, provide the MR PG logs.

Symptom 2: Activities Not Routed to Agents

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

When email activities are sent to Unified CCE by EAAS for routing, Unified EIM expects a DO_THIS_WITH_TASK message with an available agent’s ID for successfully routing the email activity to an agent. When Unified CCE sends a NEW_TASK_FAILURE message instead of a DO_THIS_WITH_TASK message, emails are not routed to agents and are instead routed to the Exception Queue.

Cause 1: Primary Unified CCE AW Database Not Configured Correctly

If the deployment only has a Primary Unified CCE Administration Workstation Database (AWDB) and the database is not running or is not configured properly, then this issue can occur.

For recommended actions for this problem, see “Cause 1: Primary Unified CCE AW Database Not Configured Correctly” on page 60.

Cause 2: Secondary Unified CCE AW Database Not Configured Correctly

If the deployment has a primary and secondary Unified CCE Administration Workstation Database (AWDB), and the primary database server becomes unavailable, the application is unable to connect to the secondary database if the secondary database is not running or is not configured properly.

For recommended actions for this problem, see “Cause 2: Secondary Unified CCE AW Database Not Configured Correctly” on page 106.

Cause 3: Unified CCE AW Database Connection Pool Limit Exceeded

There is a limit to the number of connections that can be made to the Unified CCE AWDB. If this limit exceeds the configured limit, the JDBC calls to the Unified CCE AWDB will fail and operations will terminate.

For recommended actions for this problem, see “Cause 3: Unified CCE AW Database Connection Pool Limit Exceeded” on page 106.

Cause 4: ECC Variables Not Configured Properly

This problem can happen because of issues with configuration of ECC variables and Call variables in Unified EIM and WIM and in Unified CCE.

ECC and Call variables are required for successful routing of activities. If ECC and Call variables are not correctly configured in Unified EIM and WIM and in Unified CCE, then activities will not be routed correctly to agents. Unified CCE can either completely reject the NEW_TASK_REQ messages for activities routing, or can
route activities to incorrect agents if correct ECC and Call variables are not passed as part of NEW_TASK_REQ message.

**Recommended actions:**

1. There are four required ECC variables that need to be configured in Unified CCE for successful routing of activities.
   
   user.cim.activity.id  
   user.wim.customer.name  
   user.cisco.cmb  
   user.cisco.cmb.callclass
   
   The NEW_TASK_REQ message will fail if any of these ECC variables are removed from the Unified CCE configuration or are modified in the Cisco Unified EIM & WIM configuration file.

2. The following configurations are required for email and chat routing:
   
   - Email: user.cim.activity.id ECC variable mapped to activity_id
   - Chat: user.cim.activity.id ECC variable mapped to activity_id

3. The following configurations are required for Callback and Delayed Callback routing:
   
   - user.cim.activity.id ECC variable mapped to activity_id
   - user.cisco.cmb
   - user.cisco.cmb.callclass

4. From the Administration Console, check if the correct ECC variable and Call variables are configured for the queue from which activities are not getting routed to the agents.

5. The names of the ECC variables in Unified EIM and WIM and in Unified CCE should exactly match those listed in Step 1.

6. If any ECC variable (other than the four required ECC variables mentioned in Step 1) is deleted and recreated with the same name in Unified CCE, then it needs to be remapped to queues in Cisco Unified EIM & WIM from the Administration Console.

**Cause 5: Media Router of Unified CCE Unable to Connect to EAAS Instance**

MR PIM connects to EAAS instance using a socket connection. EAAS instance runs a socket server at a port specified through the MR Connection Port property of EAAS instance configuration and System Console. MR PIM socket connection requires an IP address and a port number through which the connection is established.

Incorrect application host configuration or MR port configuration in the Unified CCE will lead to the inability of Unified CCE to successfully connect to the EAAS Instance.

**Recommended actions:**

1. From the System Console, from the EAAS instance properties, note down the value of the MR Connection Port field.

2. In Unified CCE, from the Media Routing Configuration window, look at the value of the field Application Connection Port and make sure it matches the value you noted in Step 1.
3. In the same window, verify that the value of the **Application Hostname** field is the host name or IP address of the services server of Cisco Unified EIM & WIM. You can get the host name of the services server by running the command “hostname” from the command prompt.

4. If you changed the port number, start the EAAS process and instance to reinitialize the server socket using the port number configured in Step 2.

### Cause 6: MRD Task Limit Met

The MRD task limit (also known as Queue Depth) is the maximum number of active tasks that can be queued for the given MRD (awaiting assignment) at any given instance. If this task limit has been met, no more **NEW_TASK** requests will be sent to Unified CCE, until the total number of active tasks becomes less than the MRD task limit.

**Recommended actions:**

1. Increase the MRD task limit in Unified CCE based on anticipated influx of email activities.
2. Reduce the time specified in the Unified CCE Script wait node. This ensures that the available agents are selected quickly, or the Unified CCE Script is executed within a shorter time.
3. Increase the concurrent task limit of the agents. It allows them to work on higher number of activities at one time and ensure that more agents are available at any given time.
4. From the real-time view of the CTI server, ensure that the agent availability states are accurate.

### Cause 7: Unified CCE Script Selector Not Configured Properly

An error in the configuration of Unified CCE Script Selector in the Unified EIM & WIM Administration Console (queue properties) or in Unified CCE will lead to activities not being redirected to the correct Unified CCE Script, and will impact agent assignment.

**Recommended actions:**

1. Verify that the Unified CCE Script Selector for the given MRD exists in Unified CCE, and has been associated with the Call Type, which in turn has been associated with the target Unified CCE Script.
2. In Unified EIM & WIM, verify that the queue that maps to the given MRD, has the same script selector selected.

### Cause 8: Unified CCE Script Not Configured Properly

Errors in configuring the Unified CCE Script will lead to routing of emails to unintended targets or no routing, both of which will impact agent assignment. Various issues in the Unified CCE scripts can lead to failure in activity assignment.

Some commonly observed issues for Unified CCE script are:

- Nodes of the script are not connected in accordance with intended routing.
If wait nodes are present in the script, then (real time) activities queued in Unified CCE after the wait period will be abandoned by Unified EIM and WIM, based on watchdog time intervals in `EGPL_CONFIG_PROPERTY` table of active database. To find the current value of the watchdog time interval, run the following query on the active database:

```
Select value from EGPL_CONFIG_PROPERTY WHERE DOMAIN = 'ipcc.egicm_configuration.properties' AND NAME = 'CHAT_WATCHDOG_INSEC'
```

Skill Groups configured in the Unified CCE Script are not correctly associated with their respective MRDs in Unified CCE.

**Recommended actions:**

1. Send an email activity into Unified EIM & WIM and enable Unified CCE Script monitor to trace the path of the activity after it reaches the Unified CCE Script.

2. Ensure that the nodes of the Unified CCE script are well connected, and that the flow of activities through the Unified CCE script is as intended (using Unified CCE script monitor). The Unified CCE scripts can be validated using the **Validate Script** option. Also, the call can be traced using a Call Tracer.

3. Verify that there are no long waiting nodes. The time configured for the wait nodes should be lesser than the watchdog termination time interval in Unified EIM & WIM.

4. Ensure that the MRD used for queuing an activity has respective Skill Groups included in the Unified CCE Script as targets.

**Cause 9: Concurrent Task Limit of Agent Met**

The concurrent task limit of an agent per MRD is defined as the maximum number of concurrent activities that an agent can work on in that MRD. The agent concurrent task limit is set at the queue level in Unified EIM & WIM (default=1). If this concurrent task limit is met, the agent will be unavailable for future assignment, until the agent load is lesser than the agent’s concurrent task limit.

**Recommended actions:**

1. Increase the concurrent task limit based on anticipated higher influx of emails.

2. Enable agents to work faster on existing/assigned emails.

3. Verify that the concurrent task limit in Cisco Unified EIM & WIM matches what is seen from the real-time view of agent load in Unified CCE. If there is a concurrent task limit mismatch, report this to Cisco TAC.

**Cause 10: Media Class Not Configured Properly**

The Media Class configured in Unified CCE must match the names configured in the `EGPL_Config_Property` table of the active database. If the Media Classes don’t exist in Unified CCE or there is mismatch between the names configured in Unified CCE and Unified EIM & WIM, **NEW_TASK_FAILURE** will be returned for activity routing requests.

**Recommended actions:**

1. Verify that the necessary Media Classes have been configured in Unified CCE. Ensure that the following four media classes (exact names) are configured in Unified CCE:

   ```
   CIM_WIM
   ```
2. In Unified EIM & WIM, run the following query on the active database to check the names of the Media Class.

```sql
SELECT * FROM EGPL_CONFIG_PROPERTY WHERE DOMAIN = 'ipcc.egicm_media_class_mappings.properties'
```

Ensure that the names match those configured in Unified CCE, listed here:

- **Cisco_Voice** = 9001
- **CIM_WIM** = 9002
- **CIM_EIM** = 9003
- **CIM_OUTBOUND** = 9005

3. If the names do not match, run the following query:

```sql
UPDATE EGPL_CONFIG_PROPERTY SET NAME = 'NEWNAME' WHERE NAME = 'OLDNAME' AND DOMAIN = 'ipcc.egicm_media_class_mappings.properties'
```

### Symptom 3: NIPTA Routing is Not Working

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

NIPTA (Non ICM Picks The Agent) Agents are not receiving activities through NIPTA Routing.

### Cause 1: NIPTA Routing Disabled

The NIPTA Routing setting is disabled by default. Ensure that NIPTA Routing is enabled in the database.

**Recommended actions:**

1. Verify the setting is still enabled. Run the following query on the active database:

```sql
SELECT VALUE FROM EGPL_CONFIG_PROPERTY WHERE DOMAIN = 'ipcc.egicm_configuration.properties' AND NAME = 'NIPTA_ROUTING_ENABLED'
```

2. If the result is "false", then NIPTA routing is disabled. You must enable it using the following query:

```sql
UPDATE EGPL_CONFIG_PROPERTY SET VALUE = 'true' WHERE DOMAIN = 'ipcc.egicm_configuration.properties' AND NAME = 'NIPTA_ROUTING_ENABLED'
```

3. You will need to restart the application for this to take effect.
Cause 2: NIPTA Agents Not Mapped to User Groups in Unified EIM & WIM

The NIPTA agent has not been mapped to a user group. NIPTA Routing requires the agent be a member of a user group.

Recommended actions:
1. Access the user group section of the Administration Console and check to see that the NIPTA agent have been selected for their user groups.
2. Ask the agents to log out and log back in again and verify that the activities are routed to the NIPTA Agents.

Cause 3: Unified CCE Script Labels Not Configured Correctly

Labels in Unified CCE scripts should be in the format LBL_Empire_Name_of_NonIPTA_Skill_Group. If labels in Unified CCE scripts are not configured in this format, Unified EIM & WIM will not be able to route activities to the NIPTA agent when the label is returned.

Recommended actions:
1. Verify that the correct label is returned by Unified CCE.

   In the PGA1A logs, when an activity is returned to Unified EIM & WIM for routing, we should see a DO_THIS_WITH_TASK message logged with a label that has the same name as the label associated with the NIPTA skill group to which the agent belongs.

   ```
   Message - DO_THIS_WITH_TASK: Length = 107 bytes
   DialogualId = 10000010001000003
   SeqNum = 0 Hex 00000000
   ConfigId = 1525410863: 4
   SkillGroup = Undefined
   Service = 8010 Hex 00011396
   Agent = Undefined
   Label: LBL_CIM_Email_MRD.NIPTA
   ApplicationString2:
   Call Variable 1:
   Call Variable 2:
   Call Variable 3:
   Call Variable 4:
   Call Variable 5:
   Call Variable 6:
   Call Variable 7:
   Call Variable 8:
   Call Variable 9:
   Call Variable 10:
   SOO Variable Name1 user.cim.activity.id
   Value: 1009
   00:1B:84:01:00:00:00:00 pmsg Trace: MR_Peripheral::Send_405_ServiceEstablished
   00:1B:84:01:00:00:00:00 pmsg Trace: Call 10-5, PreviousTask! TaskGroupHigh-151391, TaskGroupLow-385, SequenceNumber-1, SkillGroup=4
   00:1B:84:01:00:00:00:00 pmsg Trace: MR_Peripheral::Send_405_ServiceCleared: CallID-5, Cause=41.
   00:1B:84:01:00:00:00:00 pmsg Trace: ExpnadedCall::ContactInfo
   00:1B:84:01:00:00:00:00 pmsg Trace: MR_Dialogue::DisplayMismatchOut m_DialogHashIndex -1.
   Sample DO_THIS_WITH_TASK message
   ```

   In the example above, the returned label has the name LBL_CIM_Email_MRD.NIPTA which is the correct label for this agent’s mapped group.

   2. Reconfigure the label in the Unified CCE script.

Symptom 4: Activities Routed to Incorrect Agents

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.
Cause: Media Router Responds to NEW_TASK Without An Agent ID

When email activities are sent to Unified CCE by EAAS for routing, Unified EIM expects a DO_THIS_WITH_TASK message with an available agent’s ID for successfully routing the email activity to an agent. The DO_THIS_WITH_TASK message should contain a valid Unified CCE agent ID for email activity assignment. If no free agent is available for routing or the concurrent task limit of all the active agents is exceeded, the MR can respond to NEW_TASK with DO_THIS_WITH_TASK with a label and no agent ID.

A DO_THIS_WITH_TASK message returned with a label triggers a NIPTA (Non ICM Picks The Agent) assignment and not the expected IPTA (ICM picks the agent) assignment. When Unified CCE does not send a DO_THIS_WITH_TASK message but sends a DO_THIS_WITH_TASK with a label (without an agent ID), emails are not routed to the correct agents.

Recommended actions:
1. Identify the MRD and Script Selector for which the DO_THIS_WITH_TASK message is returned with a LABEL. Obtain this information from the NEW_TASK message in Unified CCE.
2. Go to the Unified CCE Configuration manager and select the Skill group explorer. Note down the corresponding skill groups for the specified MRD.
3. Go to the Unified CCE Configuration manager and select the Agent explorer. Find the agent associated with the above identified skills groups.
4. Go to the Unified CCE script editor and check the “IA” column. If this is 0, there is no available agent.
5. Verify the concurrent task limit of agents from the Administration Console. This is done from the Concurrent task limit tab of the queue. Consider increasing the concurrent task limit of the agents.

Symptom 5: Agent Unable to Create Outbound Emails

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

When the agent uses a new activity shortcut to create an outbound email, the outbound email does not get created. The agent sees the following error message:

You are not logged into an Outbound Media Routing Domain. Please contact your administrator for more details.

Cause: Agent Not Configured For Outbound MRD

The agent who is trying to create the outbound email might not be configured for an outbound MRD. If that is the case, the agent will not be able to create outbound emails.

Recommended actions:
1. Run the following query on the active database to get the user ID of the agent who is not able to create outbound emails.

   Select user_id from egpl_user where user_name = User Name

2. Run the following query on the active database:

   select * from egicm_user_outbound where user_id = User ID
This query displays which agent is logged in to the outbound MRD. For a logged in user, the Login_flag column shows the value 1.

3. From the Unified CCE Configuration Manager’s Agent Explorer, check if the agent is associated with an outbound MRD.

4. If the agent is not added to an outbound MRD, add the agent. From the Agent Console, try to create an outbound activity.

Symptom 6: Agent Sees Error About Completing Non-Interruptible Activities

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

When an agent tries to create an outbound activity, the following error message is displayed:

Please complete all non-interruptible activities before you attempt to create an outbound email activity.

Cause: Outbound MRD Interrupted for Agent

If the agent is working on non-interruptible activities like Callback activities, the outbound MRD will be interrupted. When the agent is working on non-interruptible activities and they try to create an outbound email, the listener service instance checks the interruptibility state of the outbound MRD and displays the error message to the agent.

Recommended actions:
1. Run the following query on the active database to get the user ID of the agent who is getting this error message.

   Select user_id from egpl_user where user_name =  \text{User Name}  

2. Run the following query on the active database to verify if callback or non-interruptible chat activities are assigned to the agent and they are still open.

   Select * from egpl_casemgmt_activity where assigned = \text{User ID} and activity_status!= 9000  

   From the query results, locate the activities with activity_sub_type 2004, 2002, 2001. If there are any such open activities, it indicates that the outbound MRD will be interrupted and the user will not be allowed to create outbound emails.

3. Complete the callback or non-interruptible chat activities assigned to the agent from the Agent Console and try to create the outbound activity.

Symptom 7: Agent Sees Maximum Number of Outbound Activities Error

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

When an agent tries to create an outbound activity, the following error message is displayed:

You have met the maximum permissible number of outbound activities that can exist in your inbox. Please complete some activities before you attempt this operation.
**Cause: Agent Concurrent Task Limit Met**

The concurrent task limit for each agent in the Outbound MRD is defined in the queue configuration from the Administration Console. This concurrent task limit defines the maximum outbound activities an agent can create. If the agent has met the concurrent task limit for a particular queue, then he will not be able to create new outbound activities.

**Recommended actions:**

1. First, identify the queue for which the agent is not able to create outbound activities. For this, go to the Agent Explorer in Unified CCE Configuration Manager, and then identify the skill groups with which the agent is associated.

2. Then go to the Skill Group Explorer in Unified CCE Configuration Manager, and find out the MRDs with which these skill groups are associated. Identify the outbound MRD and its MRD ID from the list of MRDs. The outbound MRD will be the MRD which is associated with an Outbound Media Class.

3. Run the following query on the active database to get the name of the queue mapped to the outbound MRD.

   ```sql
   select queue_name from EGPL_ROUTING_QUEUE where queue_id = (select queue_id from egicm_queue where mrd_id = <MRD_ID>)
   ```

4. Once you have identified the queue, find the concurrent task limit for the agent. You can check this from the Concurrent Task Limit tab of the queue properties from the Administration Console.

5. Match this concurrent task limit with the number of activities in the inbox of the agent. If the number of activities are equal to the concurrent task limit, complete some activities or increase the concurrent task limit allowed for a queue.

6. If you change the concurrent task limit for the queue, then log out and log in the agent again and see if he can create new activities.

**Symptom 8: Email Activities Assigned After Long Delay**

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

**Cause: OFFER_TASK_IND Message Sent After Delay**

When a **DO_THIS_WITH_TASK** message is received for a **NEW_TASK** from Unified CCE, Unified CCE expects the **OFFER_TASK_IND** message within a configured time. If this message is not received from the listener service instance in Unified EIM and WIM, Unified CCE makes the agent non-routable and sends the **AGENT_MADE_NOT_ROUTABLE_EVENT** message to the listener service instance. In response, the listener service sends the **MAKE_AGENT_ROUTABLE** message to make the agent routable immediately. All **OFFER_TASK_IND** messages sent during this time will be rejected by Unified CCE and a **FAILURE_RESP** message from Unified CCE is dispatched. The Unified EIM and WIM listener instance then enables email activity for re-routing to Unified CCE.

If this scenario continues for many activities, the activities for which the **OFFER_TASK_IND** message was not received within a configured time are assigned after a long delay.
Recommended actions:

1. Locate the `AGENT_MADE_NOT_ROUTABLE_EVENT` message in the CTI server logs. If this message is found, it indicates that the `OFFER_TASK_IND` message for the email activity would have been rejected at Unified CCE. The Listener will immediately send the `MADE_AGENT_ROUTABLE` message to Unified CCE.

2. In the CTI server logs, locate the `FAILURE_RESP` message. In the message, note down the `DialogueID`. In the CTI logs, look for the `OFFER_TASK_IND` message for the same `DialogueID`. This tells that a failure had occurred and it was recovered internally. From the `OFFER_TASK_IND` message, get the `Task ID`.

3. Use this `Task ID` to locate the previous `NEW_TASK` message in the MR PG logs. Note the activity ID mentioned in the `NEW_TASK` message. Verify that there is another `NEW_TASK` message with the same activity ID.

4. From the `NEW_TASK` message get the `MRD ID`.

5. If this problem is happening continuously, check if there are any network connection issues between the various servers. If you find such issues, fix them and see if the problem is fixed.

6. If there are no network issues, find the MRD related to the `MRD ID` by running the following query on the Unified CCE AWDB.

   ```sql
   select * from t_Media_Routing_Domain where MRDomainID = MRD_ID
   ```

7. From the Unified CCE Configuration Manager, from the Media List properties, increase the value of the `Start timeout` setting. When a `DO_THIS_WITH_TASK` message is received for a `NEW_TASK` from Unified CCE, Unified CCE expects the `OFFER_TASK_IND` message within this configured time.
Chat Issues

- Chat Assignment Issues
- Chat Session Issues
This chapter describes recommended actions for the most common issues related to chat.

**Chat Assignment Issues**

**Symptom 1: Delay in Chat Assignment**

Chats are not assigned to agents instantly. Chats do get assigned, but there is some delay between the time the customer starts the session and the chat is assigned to an agent.

**Cause 1: All Agents Have Reached Maximum Load**

All agents who can service chats have reached their maximum load and no new chats can be assigned to the agents.

**Recommended actions:**

1. From the Administration Console, check the value set for the setting **Chat- User Max Load**. The setting is available at the department and user level. Modify this if required.

2. From the Supervision Console, set up a monitor with the following attributes and validate that there are agents available to whom the chat activity can be assigned and the agent’s current load is less than the maximum allowed chat load.

   - For queue: **Chat - Number in progress**, **Chat- Number not started**, **Chat - Number of agents available**, **Chat - Number unassigned**.
Cause 2: Activities Pushed Back to Queue

The chat was assigned to an agent, but got pushed back to the queue. The application is designed such that if an agent does not select the chat activity within the time configured in the **Expiry Time for Auto-Pushback for Chats (Minutes)** setting, the chat is automatically pushed back to the queue so that it can be reassigned. The default value for auto-pushback of chat activities is 2 minutes.

For integrated chats, the chat activity is re-routed for agent assignment through EAAS. In Unified CCE, the current task for the activity is ended and the agent made unavailable for any new chats until they explicitly make themselves available from the Agent Console.

Please refer to the *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Administration Console*, “Chat Auto-Pushback Settings” section for more information.

**Recommended actions:**

1. Check the Auto-Pushback settings for chat from the Administration Console. If Auto-Pushback is enabled, check the value of the **Expiry Time for Auto-Pushback for Chats (Minutes)** setting.

2. Get the audit information for the activity by running the following query on the active database.

   ```sql
   select cast(dateadd(ss,event_date/1000,'1/1/1970')as datetime),* from egpl_event_history_case_mgmt where activity_id = <ACTIVITY_ID> order by event_date
   ```

   In the activity audit trail, check if there is an event `object_operation 308`. It indicates that the activity was pushed back to the queue before an agent selected it. This is the expected behavior and is meant to ensure that customers are not kept waiting endlessly for an agent.
Perform the following additional tasks for integrated chats:

3. From the MR logs or from the egicm_activity table in the Cisco Unified EIM & WIM active database, identify the task ID for the activity which was pushed back to the queue. Run the following query on the active database to get the task ID:

   ```sql
   select Task_group_high+task_group_low+sequence_number as task_id from egicm_activity where activity_id = Activity_ID
   ```

4. Verify from the CTI server logs that there is an END_TASK_IND message for the task ID. Failure in sending the END_TASK_IND will lead to activity mismatch between Unified CCE and Unified EIM and WIM.

5. Agent should be made unavailable in Unified CCE by sending the MAKE_AGENT_NOT_ROUTABLE and MAKE_AGENT_NOT_READY massages to CTI server. Verify the same in the CTI server logs for the agent.

6. Check for activity re-routing. Verify that there is a new NEW_TASK request in MR logs for the same activity ID. Look for the activity ID in the NEW_TASK message. If there are two or more NEW_TASK messages with the same activity ID, it means the activity has been re-routed.

### Further Actions

If none of the above mentioned recommended actions solve your problem, then collect data using the following tools and send the information to Cisco TAC.

1. Get the HTTP or Fiddler trace logs for the Chat Customer Console. For details on running these tools, see “Troubleshooting Tools” on page 20.

2. From the Tools Console, access the Utilities window and run the Debug Agent Assignment Service utility to log the current state of the service. The utility logs the information in the log file:

   ```
   eg_log_Services_Server_Name_agent-assignment-process.log
   ```

   The log file is available at Cisco_Home\eService\logs on the services server.

3. Get the `eg_log_Services_Server_Name_agent-assignment-process.log` log file for the Agent Assignment Service.

4. Get the access logs `Application_Server_Name_access_log.Date.log` for the agent and the customer. In a load balanced environment, you need to first identify the server where the customer or agent is connected.

   To find the application server where the customer is connected to, run the following query on the active database and get the information from the `attendee_home` column:

   ```sql
   select activity_id, attendee_home from eglv_attendee where activity_id = Activity_ID and agent = 0
   ```

   To find the application server where the agent is connected to, run the following query on the active database and get the information from the `attendee_home` column:

   ```sql
   select activity_id, attendee_home from eglv_attendee where activity_id = Activity_ID and agent = 1
   ```

5. Get the `eg_log_Application_Server_Name_ApplicationServer.log` and `egpl_root_Application_Server_Name.log` log files for the agent and customer application servers.

6. From Unified CCE, get the CTI Server and MR logs.

7. Run the following queries on the active database and get all the details for activities that are getting assigned after a delay.
Symptom 2: Chats Not Assigned to Agents

The chat queue is configured to push chats to agents, but the chats are not getting assigned to agents. The activities do not appear in the agent’s inbox. This could happen for the following reasons.

Cause 1: Primary Unified CCE AW Database Not Configured Correctly

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

If the deployment only has a primary Unified CCE Administration Workstation Database (AWDB), and the database is not running or not configured properly, this issue can occur.

For recommended actions for this problem, see “Cause 1: Primary Unified CCE AW Database Not Configured Correctly” on page 60.

Cause 2: Secondary Unified CCE AW Database Not Configured Correctly

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

If the deployment has a primary and secondary Unified CCE Administration Workstation Database (AWDB), and the primary database server becomes unavailable, the application is unable to connect to the secondary database if the secondary database is not running or is not configured properly.

For recommended actions for this problem, see “Cause 2: Secondary Unified CCE AW Database Not Configured Correctly” on page 60.

Cause 3: Unified CCE AW Database Connection Pool Limit Exceeded

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

There is a limit to the number of connections that can be made to the Unified CCE AWDB. If this limit exceeds the configured limit, the JDBC calls to the Unified CCE AWDB will fail and operations will terminate.
For recommended actions for this problem, see “Cause 3: Unified CCE AW Database Connection Pool Limit Exceeded” on page 120

**Cause 4: Queues Not Configured to Route Chats**

The queue properties have not been configured properly to route chats to agents.

**Recommended actions:**

1. Identify the ID of the entry point from which activities have issues. You can do it by viewing the source of the entry point and searching for `entryPointId=`. The value for this property is the entry point ID. For example, in `entryPointId=1000`, the entry point ID is 1000.

2. Get the queue used in the chat entry point by running the following query:

   ```sql
   select queue_name, EGLV_ENTRY_POINT.QUEUE_ID from EGLV_ENTRY_POINT, EGPL_ROUTING_QUEUE where entry_point_id = Entry_Point_ID and EGPL_ROUTING_QUEUE.QUEUE_ID = EGLV_ENTRY_POINT.QUEUE_ID
   ```

3. In the Administration Console, browse to Administration > Department > Department_Name > Workflow > Queues, and for the queue, check the value of the Chat push routing method field. The value should be Load balanced. Also, ensure that correct users and user groups are selected for receiving chats.

**Cause 5: Queue Not Mapped to Correct MRD**

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

The queue configured for routing chat activities in Unified WIM is not mapped to the correct MRD.

**Recommended actions:**

1. Launch the application. Log in as an administrator and go to the Administration Console.

2. Browse to Administration > Department > Department_Name > Workflow > Queues.

3. In the List pane, select the queue configured for chat activities.

4. In the Properties pane on the General tab, check the value configured in the Media Routing Domain field. The value should be set to a chat MRD.

**Cause 6: Agents Unavailable to Receive Chats**

The agent has not set the Availability setting correctly to receive chats.

**Recommended actions:**

1. From the Supervision Console, setup a monitor for the chat queue with the following attributes and validate that there are agents available to whom chats can be assigned.

   - For queue: Chat - Number in progress, Chat- Number not started, Chat - Number of agents available, Chat - Number unassigned.
2. From the Agent Console, check the availability setting of the agents.

**Cause 7: All Agents Have Reached Maximum Load**

All the agents who can service chats have reached their maximum load and no new chats can be assigned to the agents. As a result, chats are waiting in the queue for assignment.

**Recommended actions:**

- For recommended actions for this problem, see “Cause 1: All Agents Have Reached Maximum Load” on page 117.

**Cause 8: Script Error Occurs in the Agent Console**

Agents are unable to receive chats because an Internet Explorer script error occurs while logging in, or while chats are assigned to agents.

**Recommended actions:**

1. Enable the script error notifications for Internet Explorer and log in to the Agent Console again. For details on enabling script error notifications, see “Troubleshooting Tools” on page 20.

2. If the issue is consistent, collect the Script Debugger logs and screenshots of the Agent Console and pass the information to Cisco TAC for further troubleshooting.
Cause 9: Problems With Agent Assignment Service

The activity is not assigned by the Agent Assignment service to any agent even though the queue is configured properly, agents are available for receiving chats, and agents have not reached their maximum load.

Recommended actions:

1. Identify the ID of the entry point from which activities have issues. You can do it by viewing the source of the entry point and searching for `entryPointId=`. The value for this property is the entry point ID. For example, in `entryPointId=1000`, the entry point ID is 1000.

2. To find the activities that are not getting assigned to an agent for the entry point, run the following query on the active database:

   ```sql
   select activity_id, assigned_to
   from EGLV_ENTRY_POINT, EGPL_ROUTING_QUEUE, EGPL_CASEMGMT_ACTIVITY
   where entry_point_id = Entry_Point_ID
   and EGPL_ROUTING_QUEUE.QUEUE_ID = EGLV_ENTRY_POINT.QUEUE_ID
   and EGLV_ENTRY_POINT.QUEUE_ID = EGPL_CASEMGMT_ACTIVITY.queue_id
   and EGPL_CASEMGMT_ACTIVITY.activity_status = 4000
   and EGPL_CASEMGMT_ACTIVITY.activity_sub_status = 4100
   ```

3. Validate that the activity has not been assigned to an agent from the activity audit in the database. If the `object_operation 203` event is not logged for this activity, it indicates that the activity was not assigned to any agent by the Agent Assignment service. To get the audit information for an activity, run the following query on the active database:

   ```sql
   select cast(dateadd(ss,event_date/1000,'1/1/1970')as datetime), * from egpl_event_history_case_mgmt where activity_id = Activity_ID order by event_date
   ```

4. From the System Console, stop and start the Agent Assignment service. Check if the chat assignment is working after the service is restarted.

Cause 10: Problems With JMS Messaging

There is some problem with messaging between the services server which hosts the Agent Assignment Service, and the application server.

Recommended actions:

1. Identify the ID of the entry point from which chat activities are failing. You can do this by viewing the source of the entry point and searching for `entryPointId=`. The value for this property is the entry point ID. For example, in `entryPointId=1000`, the entry point ID is 1000.

2. To find the activities that are not getting assigned to an agent for the entry point, run the following query on the active database:

   ```sql
   select activity_id, assigned_to
   from EGLV_ENTRY_POINT, EGPL_ROUTING_QUEUE, EGPL_CASEMGMT_ACTIVITY
   where entry_point_id = Entry_Point_ID
   and EGPL_ROUTING_QUEUE.QUEUE_ID = EGLV_ENTRY_POINT.QUEUE_ID
   and EGLV_ENTRY_POINT.QUEUE_ID = EGPL_CASEMGMT_ACTIVITY.queue_id
   ```
and EGPL_CASEMGMT_ACTIVITY.activity_status = 4000
and EGPL_CASEMGMT_ACTIVITY.activity_sub_status = 4100

3. Validate that the activity has not been assigned to an agent from the activity audit in the database. If the
object_operation 203 event is not logged for this activity, it indicates that the activity was not assigned
to any agent by the Agent Assignment service. To get the audit information for an activity, run the following
query on the active database:

```sql
select cast(dateadd(ss,event_date/1000,'1/1/1970')as datetime), * from
egpl_event_history_case_mgmt where activity_id = Activity_ID order by event_date
```

4. Access the URL:


   a. From the Select API to view the details dropdown list, select

      `getassignedactivityDetailsForMonitoring(activityid)` and in the ActivityID field provide the ID of
      the activity.

   b. If the debug JSP output indicates that the activity is assigned to a user, that is the assignedTo
      property displays a user ID, it means that the activity was assigned by the Agent Assignment Service but the
      Application Server failed to receive the assigned activity message.

5. JMS is not working. Check if there are any JMS related exceptions in the following log files:

   eg_log_Application_Server_Name_ApplicationServer.log
   eg_log_Services_Server_Name_agent-assignment-process.log

Look for the following messages:

- org.jboss.mq.SpyJMSException: Exiting on IOE; - nested throwable:
  (java.net.SocketTimeoutException: Read timed out)

- org.jboss.mq.SpyJMSException: Cannot send a message to the JMS server; - nested throwable:
  (java.io.IOException: Client is not connected)

- org.jboss.mq.SpyJMSException: Exiting on IOE; - nested throwable:
  (java.net.SocketException: Connection reset)

- javax.naming.CommunicationException [Root exception is
  java.rmi.ConnectException: Connection refused to host: <Messaging Server>

- org.jboss.mq.SpyJMSException: No pong received; - nested throwable:
  (java.io.IOException: ping timeout.)

- Error in publishing message to destination:

- Failed to publish message to destination:

- Failed to Subscribe to JMS destination

- Error in creating messageObject for destination

- Exception in refreshHandles()

- OnException invoked on connection

- Failed to establish Connection on attempt number:
Cause 11: Problems With Event Messaging

 Occasionally, activity assigned to an agent by the Agent Assignment Service does not appear in the agent’s inbox due to a problem with event messaging.

Recommended actions:

1. Identify the ID of the entry point from which activities are not appearing in the agent’s inbox. You can do it by viewing the source of the entry point and searching for entryPointId=, The value for this property is the entry point ID. For example, in entryPointId=1000, the entry point ID is 1000.

2. To find the activities that are assigned to an agent for the entry point, run the following query on the active database:

   ```sql
   select activity_id, assigned_to
   from EGLV_ENTRY_POINT, EGPL_ROUTING_QUEUE, EGPL_CASEMGMT_ACTIVITY
   where entry_point_id = Entry_Point_ID
   and EGPL_ROUTING_QUEUE.QUEUE_ID = EGLV_ENTRY_POINT.QUEUE_ID
   and EGLV_ENTRY_POINT.QUEUE_ID = EGPL_CASEMGMT_ACTIVITY.queue_id
   and EGPL_CASEMGMT_ACTIVITY.activity_status = 5000
   ```

3. Validate that the activity has been assigned to an agent from the activity audit in the database. If the object_operation 203 event is logged for this activity, it indicates that the activity was not assigned to any agent by the Agent Assignment Service. To get the audit information for an activity, run the following query on the active database:

   ```sql
   select cast(dateadd(ss,event_date/1000,'1/1/1970')as datetime),* from egpl_event_history_case_mgmt where activity_id = Activity_ID order by event_date
   ```

4. In case the activity is already assigned to the user as per the activity audit, get the user_id from the activity audit and check for polling requests from the Agent Console to the application server, and check the response code for these requests. This can be checked from Fiddler or Http trace if available, or from the agent’s application server access logs. For details about the access logs, see “Further Actions” on page 119. For using the Fiddler or Http tools, see “Troubleshooting Tools” on page 20.

   Look for:

   ```
   Format: GET http://Server_Name/Context_Root/mr_pushlet.egain
   ```

   For example:

   ```
   Format: GET http://company_server/system/mr_pushlet.egain
   ```

5. From the Agent Console, log out and log in again. If the assigned chat activity appears, check if the chat message exchange between the agent and customer is working by sending a few chat messages.

6. If the chat message exchange is not working check if the instant messaging is working. To check this, do the following:

   a. Log in to Agent Console and from the Console toolbar, check if the Messages button indicates unread messages. Then, check the Messages window to make sure there are no unread messages.

   b. Now, send a message to this user from another user login and check if the Messages button indicates a new message has arrived.

   If the Messages count is updated instantly, it indicates that instant messaging is working.
Further actions

If none of the above mentioned recommended actions solves your problem, then collect data using the following tools and send the information to Cisco TAC.

- Collect all the information listed in “Further Actions” on page 119 and send it to Cisco TAC.
- From the Tools Console, access the Utilities window and run the Debug Agent Assignment Service utility to log the current state of the service. The utility logs the information in the log file: `eg_log_services_server_Name_agent-assignment-process.log`. The log file is available at `Cisco_Home\eService\logs` on the services server. Get the `eg_log_service_Server_Name_agent-assignment-process.log` file.

Chat Session Issues

Symptom 1: Error Message Displayed When Chat Agent Logs In

Agents get the following message after login:

The system encountered an error due to which the assignment of chats to your inbox has been disabled. If you need to handle chat activities during this session, please log out and then log in again.

This error occurs when the Agent Console takes more than 150 seconds (two and a half minutes) to load.

Recommended actions:

1. Check the following guides and validate that the agent’s desktop has the correct Internet Explorer version and all the browser settings have been configured properly. If not, correct these and check if the issue is fixed after making these changes.
   - Cisco Unified Web and E-Mail Interaction Manager System Requirements
   - Cisco Unified Web and E-Mail Interaction Manager Browser Settings Guide
2. Log out and log in again and confirm that in the next login the agent does not get the same message.
3. If the issue is consistent, collect all the information listed in “Further Actions” on page 119 and send it to Cisco TAC.
Symptom 2: Service Unavailable Message Displayed

When a customer tries to initiate a chat, the customer sees the service unavailable template. This can occur for one of the following reasons.

Cause 1. Entry Point Not Active

If the entry point is not active, customers will not be able to start chat sessions.

Recommended actions:

1. Identify the ID of the entry point from which activities have issues. You can do it by viewing the source of the entry point and searching for `entryPointId=`. The value for this property is the entry point ID. For example, in `entryPointId=1000`, the entry point ID is 1000.

2. Run the following query for the entry point ID identified in Step 1:
   ```
   select * from eglv_entry_point where entry_point_id = Entrypoint_ID
   ```

3. In the query results, check the value in the column `is_active`. If the value is 0 it indicates that the entry point is not active. Get the entry point name from the query results.

4. In the Administration Console, browse to Administration > Department > Department_Name > Entry Point, and check if the entry point is active. If not, make the entry point active.

Cause 2. Agents Not Available

Agents are not available to receive chats.

Recommended actions:

1. In the Administration Console, browse to Administration > Department > Department_Name > Entry Point, and check if the agent availability is required for creating chats for this entry point.

2. For the queue used in the entry point, check if load balancing has been enabled for chats. This can be checked from the Queue node in the Administration Console. For load balanced queues, check if correct users and user groups are selected in the Chat tab of the queue. Using monitors from the Supervision Console, check if at least one of the agents selected in the Chat tab is logged in and available for chats.

3. If agents are required to pull activities from queues, then make sure that agents have correct permissions on the chat queues. This can be checked from the queue, user, or user group properties from the Administration Console. Using monitors from the Supervision Console, check if at least one agent with pull permissions on the chat queue is logged in and available for chat.

   From the Supervision Console, setup a monitor for the chat queue with the following attributes:

   - For queue: Chat - Number in progress, Chat- Number not started, Chat - Number of agents available, Chat - Number unassigned.
For agent: User name, Chat - Available to handle, Chat - Number in progress, Chat - Number not started

Sample chat monitor

**Cause 3. Agent Assignment Service Not Started**

The Agent Assignment Service for chat is stopped or is experiencing a problem.

**Recommended actions:**

- From the System Console, stop and start the Agent Assignment service. Check if the problem is resolved after the service is restarted.

**Cause 4: EAAS Service Not Started**

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

The EAAS Service is stopped or is having a problem.

**Recommended actions:**

- From the System Console, stop and start the EAAS process and instance. Check if the problem is resolved after the service is restarted.
**Cause 5: Chat Queueing Disabled For Integrated Chat Agents**

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

Chat Queueing is disabled in the system and customers are displayed the off-hours template when initiating chat, even though the IPTA and NIPTA chat agents are logged in and available for chat. By default, Chat Queueing is enabled in the system.

**Recommended actions**

1. Verify that the Chat Queueing setting is still enabled. To check the current value of the setting, run the following query on the active database:

   ```sql
   SELECT VALUE FROM EGPL_CONFIG_PROPERTY WHERE DOMAIN = 'ipcc.egicm_configuration.properties' AND NAME = 'ENABLE_CHAT_QUEUING'
   ```

2. If the result is “false”, then the setting is disabled. You must enable it using the following query:

   ```sql
   UPDATE EGPL_CONFIG_PROPERTY SET VALUE = 'true' WHERE DOMAIN = 'ipcc.egicm_configuration.properties' AND NAME = 'ENABLE_CHAT_QUEUING'
   ```

3. You will need to restart the application for this to take effect.

**Further actions**

If none of the above mentioned recommended actions solve your problem, then collect the following log files and send the information to Cisco TAC.

- From the Tools Console, access the Utilities window and run the Debug Agent Assignment Service utility to log the current state of the service. The utility logs the information in the log file: `eg_log_services_server_Name_agent-assignment-process.log`. The log file is available at `Cisco_Home\eService\logs` on the services server. Get the `eg_log_services_server_Name_agent-assignment-process.log` file.

- `eg_log_Application_server_Name_ApplicationServer.log`

- `egpl_root_Application_server_Name.log` for all application servers

**Cause 6: EAAS Not Connected to Media Router**

The EAAS service is not able to connect to the media router.

- See “External Agent Assignment Service Issues” on page 98.

**Symptom 3: Customers see “System Cannot Assign an Agent to the Request”**

Customers get the following error message when they start a chat session: **System cannot assign an agent to the request.**
Cause: No Chat Agents Logged in to Unified EIM and WIM

A chat request enters the Unified EIM and WIM application through an entry point. Every entry point is associated with a queue that is in turn mapped to an Unified CCE Media Routing Domain (MRD) and a script selector (that is used to identify the Unified CCE script to route the chat). Integrated agents are associated with one or more MRDs in Unified CCE. If no agents associated with an integrated MRD are logged into Unified EIM and WIM, the chat activity will be abandoned. Consequently, chat assignment will fail.

Recommended actions:
1. To find the activities that are not assigned to an agent, run the following query on the active database:
   ```sql
   select activity_id from egpl_casemgmt_activity where activity_sub_status=2001 and assigned_to = -1
   ```
2. On the Unified CCE server, navigate to the MR PG logs, and verify that a NEW_TASK message exists for each of the failed chat activities. Note the dialog ID in the NEW_TASK message and locate the NEW_TASK_FAILURE message for the same dialog ID in the MR PG logs. When the EAAS instance receives this NEW_TASK_FAILURE from MR PG, the chat activities will be closed without assignment.
3. Identify the MRD ID and Script Selector for which the NEW_TASK message was sent. This information can be obtained from the NEW_TASK message.
4. In Unified CCE Configuration Manager, navigate to the Skill Group explorer. Note down the corresponding skill groups for the MRD identified in Step 3.
5. Navigate to the Agent explorer. Note the agents associated with the skills group identified in Step 4. From the Unified CCE Script Editor, check the “IA” column (this column indicates availability). If the value is 0 for all agents, then there are no available agents.
6. Have the agents login to Unified EIM and WIM and make sure they are available for chat.

Symptom 4: “Lines are Busy” Message Displayed to Chat Customers

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

After the customer starts a chat session, the “Lines are busy” message is displayed in the customer's chat window.

Cause 1: Chat Activity Abandoned by the Watchdog Thread

The EAAS instance has a Watchdog component for tracking the NEW_TASK messages sent to MR PG. The Watchdog keeps a count of the time that has elapsed since the NEW_TASK message for an activity was sent to MR PG without the DO_THIS_WITH_TASK message being received. If no DO_THIS_WITH_TASK message is received within the configured time, the Watchdog will terminate the NEW_TASK message by sending the TERMINATE_DIALOG_BOX message to MR PG. It will in turn close the chat activity in Unified EIM and WIM by abandoning it without assignment.

The chat watchdog interval is specified in the CHAT_WATCHDOG_INSEC property in the EGPL_CONFIG_PROPERTY table of the active database. To find the current value of the Watchdog time interval, run the following query on the active database:

```sql
Select value from EGPL_CONFIG_PROPERTY WHERE DOMAIN = 'ipcc,egicm_configuration.properties' AND NAME = 'CHAT_WATCHDOG_INSEC'
```
If a chat activity remains in the Unified CCE queue for more than this duration, the Watchdog thread identifies that the chat has exceeded its queuing period, and it abandons the activity. The activity is tagged as abandoned in the system and the customer is displayed the “Lines are busy” message.

**Recommended actions:**

1. Access the MR PG logs on the Unified CCE server.

2. In the log file search for the `TERMINATE_DIALOGUE_REQ` messages. A `TERMINATE_DIALOG_REQ` message is sent from the EAAS instance to the MR PG (via the MR interface) for the activity ID for which the `NEW_TASK` message is sent from EAAS to MR, but no `DO_THIS_WITH_TASK` message is received from MR. These type of activities are considered as abandoned and the watchdog terminates them by sending the `TERMINATE_DIALOG_REQ` message to MR for the dialog ID for which the `NEW_TASK` message was sent.

   For example, the message will look like:
   ```
   Message = TERMINATE_DIALOGUE_REQ; Length = 16 bytes
   DialogueID = (2) Hex 00000002
   SendSeqNo = (2) Hex 00000002
   InvokeID = (2) Hex 00000002
   Reason = (22) Hex 00000016
   ```

3. Note the dialog ID of the `TERMINATE_DIALOGUE_REQ` and locate the `NEW_TASK` message with the same dialog ID. Note the activity ID for which this `NEW_TASK` message was sent for reference. Using the activity ID, identify the Unified CCE script which is executed for the `NEW_TASK`.

4. Check if there are wait nodes with long wait times configured in this Unified CCE script, which may exceed the chat watchdog time interval configured in the `CHAT_WATCHDOG_INSEC` property in the `EGPL_CONFIG_PROPERTY` table of the active database. To find the current value of the watchdog time interval, run the following query on the active database:

   ```
   Select value from EGPL_CONFIG_PROPERTY WHERE DOMAIN = 'ipcc.egicm_configuration.properties' AND NAME = 'CHAT_WATCHDOG_INSEC'
   ```

   If long wait nodes are present, reduce the time on the wait nodes to be less than or equal to the chat watchdog time interval. Alternatively, consider increasing the chat watchdog time interval in the database using the following query to be greater than or equal to the wait node:

   ```
   UPDATE EGPL_CONFIG_PROPERTY SET VALUE = Time WHERE DOMAIN = 'ipcc.egicm_configuration.properties' AND NAME = 'CHAT_WATCHDOG_INSEC'
   ```

**Cause 2: All Integrated Chat Agents Have Reached Concurrent Task Limit**

In Unified EIM and WIM, the concurrent task limit for every agent is defined in the Queue properties in the Administration Console. This value is specified at a per MRD level indicating how many activities a given agent can work on concurrently. If this value has been met, then the agent will not receive any new activities until the current load is reduced.

**Recommended actions:**

1. In the Unified CCE Script Editor, open the real time table for a skill group, and compare the number of calls in progress for agents with the column that tells the concurrent task limit for agents.

2. If both these values are the same, you must consider increasing the concurrent task limit of the agents from the Queue properties in the Administration Console of Unified EIM and WIM.
Agents would need to log out and log back in for the changes to take effect.

**Symptom 5: Wait Template Not Displayed to Chat Customers**

This section only applies to Unified EIM and WIM systems that are integrated with Unified CCE.

The system might be configured in a way that Unified CCE sends a `RUN_APPLICATION_SCRIPT_REQ` message from the Media Router to EAAS to run a script (to show a custom template) on the Chat Customer Console before the chat assignment happens. EAAS fetches details of the script template from a Unified EIM and WIM configuration file, based on the script name in the `RUN_APPLICATION_SCRIPT_REQ` message, and then publishes this template on the Chat Customer Console. If the file is not configured properly, the wait template is not displayed to the customer and the customer is shown the message “Waiting for agent assignment.”

**Cause: Incorrect Tags Configured in DRASR Configuration File**

Attributes such as the script name that are used by the `RUN_APPLICATION_SCRIPT_REQ` message are included in the following configuration files:

- **File server:**
  ```
  Cisco_Home\eService\installation\ear\eService.ear\lib\configurations_custom.zip\ipcc\egicm_message_map.xml
  ```

- **Services server:**
  ```
  Cisco_Home\lib\configurations_custom.zip\ipcc\egicm_message_map.xml
  ```

The script names configured in these files must exactly match the script names configured in Unified CCE. If the names do not match, the `RUN_APPLICATION_SCRIPT_REQ` message from the Unified CCE MR PG will not result in the display of the custom wait template on the Chat Customer Console.

For details about configuring Dynamic Run Application Script Request (DRASR) see the “Configuring Dynamic Messages for Integrated Chats” section in the *Cisco Unified Web and E-Mail Interaction Manager Deployment and Maintenance Guide*.

**Recommended actions:**

1. Verify that the Unified CCE Script is configured to send a `RUN_APPLICATION_SCRIPT_REQUEST` message to the EAAS instance.
   a. The names provided in the **Unified CCE Configuration Manager > Network VRU Script List** should match the names provided in the `egicm_message_map.xml` file.
   b. In the Unified CCE Script, the Run External Script node should be configured with the correct script name. In addition to the script name, verify the validity of this DRASR script.

2. Verify that this script name is also configured in the **File_Server_Home\eService\installation\ear\eService.ear\lib\configurations_custom.zip\ipcc\egicm_message_map.xml** and **Services_Server_Home\lib\configurations_custom.zip\ipcc\egicm_message_map.xml**.

3. Search the `RUN_APPLICATION_SCRIPT_REQ` message in the MR PG logs. The dialog ID of the message must be the same as that of the `NEW_TASK` message for the chat activity request.

For example, the message can look like:

```
17:05:39 pg2A-pim1 Trace: PG->Application:
```
Message = RUN_APPLICATION_SCRIPT_REQ; Length = 156 bytes
DialogueID = (2) Hex 00000002
SendSeqNo = (1) Hex 00000001
InvokeID = (41) Hex 00000029
EstimatedWaitTime: Time
ScriptID: google
ECC Variable Name: user.cim.activity.id
Value: 1028

4. Verify that there is a successful response in the form of RUN_APPLICATION_SCRIPT_RESULT message from EAAS to the RUN_APPLICATION_SCRIPT_REQ message. This can be located in the MR PG logs by searching the same dialog ID that was sent for the RUN_APPLICATION_SCRIPT_REQ message. Verify the ScriptResult field in the RUN_APPLICATION_SCRIPT_RESULT message. If the ScriptResult value is 1, it implies that the script was executed successfully. If the ScriptResult value is 0, it implies that EAAS failed to execute the script.

For example, a failed RUN_APPLICATION_SCRIPT_RESULT message will look like:

Message = RUN_APPLICATION_SCRIPT_RESULT; Length = 16 bytes
DialogueID = (1) Hex 00000002
SendSeqNo = (2) Hex 00000002
InvokeID = (15) Hex 0000000f
ScriptResult = (0) Hex 00000000

Symptom 6: Customer Chat Status Changes to “Slow But Still Connected”

A yellow triangle, indicating that the customer is “Slow but still connected”, is displayed against the chat activity in the Agent Console. This can occur for connectivity issues between the application server and the Chat Customer Console.

The chat status in the Agent Console indicates the health of the connection between the application and the customer browser. In case of network connectivity issues between the customer browser and application server, the status of the chat is changed in the Agent Console from green (good connection) to yellow (slow, but still connected).

Recommended actions:

- Turn on Fiddler or HttpTrace for the Customer Console. Create another chat and see if the issue persists for the subsequent chat as well. Look for any network related errors in the requests flowing from the Chat Customer Console.

Further actions

- If the issue is consistent, collect all the information listed in “Further Actions” on page 119 and send it to Cisco TAC.
Symptom 7: Chat Messages Not Delivered to Agents or Customers

Agents or customers do not receive messages sent during the chat session.

Cause 1. Connection Issues to Application Server

This problem can occur because of connectivity issues between the application server and the Agent Console or the Chat Customer Console.

Recommended actions:
1. From the Agent Console, complete the chat activity and see if the lost messages are seen in the chat transcript available from the Completed folder.
   If the messages are not seen in the chat transcript of the completed chat, it indicates that there are network connectivity issues to the application server.
2. Turn on Fiddler or HttpTrace for Console the issue is occurring in. Create another chat and see if the issue persists for the subsequent chat as well. Look for any error responses for the requests being sent out.

Further actions
› If the issue is consistent, collect all the information listed in “Further Actions” on page 119 and send it to Cisco TAC.
› Also, get the eg_log_Service_Server_Name_agent-assignment-process.log file.

Cause 2. Problems With Event Messaging

This issue can occur when a problem with event messaging causes messages to not appear in the agent’s inbox.

Recommended actions:
› For recommended actions for this problem, see “Cause 11: Problems With Event Messaging” on page 125.

Further actions
› If the issue is consistent, collect all the information listed in “Further Actions” on page 119 and send it to Cisco TAC.

Also, get the eg_log_Service_Server_Name_agent-assignment-process.log file.
Offers Issues

- Offers Display Issues
This chapter describes recommended actions for the most common issues related to offers.

**Offers Display Issues**

**Symptom 1: Offers Not Displayed on Web Pages**

**Cause 1: Offer Enablement Code Not Added to Web Pages**

The Offer Enablement Code required for Offers to work has not been added to the web pages.

**Recommended actions:**

- The Offer Enablement code is used to enable the website for offers. As a part of deploying the application, your system administrator should have already configured the website with the Offer Enablement code. Check with your system administrator to make sure that the Offer Enablement code is added to the websites where you want to present offers.

**Cause 2: Incorrect Page URL Configured**

The web pages configured in the Offers Console are not using the correct URLs. You need to provide the exact URL or a matching URL pattern.

**Recommended actions:**

- From the Offers Console check the web page URLs configured for offers. For example, if the web page URL is `http://www.company.com/support.htm`, then provide the exact URL, `http://www.company.com/support.htm`, or a matching URL pattern, such as `.*support.*` or `*company*`.

**Cause 3: Offers Not Activated**

Offers is configured, but has not been activated. After an offer has been configured and associated with a web page, it should be activated for that web page.

**Recommended actions:**

- From the Offers Console, check if the offers associated with the web pages have been activated.
Cause 4: Eligibility Conditions Not Met

Offers are not getting displayed because the eligibility conditions configured for the offers have not been met.

**Recommended actions:**
1. From the Offers Console, check if the eligibility conditions configured for offers are being met by the website visitor.
2. Check if the offer is configured to display when any condition is met, or when all the conditions are met.

Cause 5: Chat Offers Requirements Not Met

Chat automatic offers are displayed only when the following conditions are met.

- Agent assignment service is running.
- A chat agent is logged in and available in the Agent Console.
- The current load of the chat agent is less than the maximum allowed chat load.
- If queue depth is configured for the chat queue, the queue is not full.

**Recommended actions:**
- Check the above listed conditions and make sure they meet chat automatic offers’ requirements.

Cause 6: Offer is Not Configured Relative to the Correct Object

The offer is configured relative to an object on the web page, but the Object ID configured in the offer banner is not correct, or the object is missing from the page.

**Recommended actions:**
1. From the Offers Console, check if the position selected for the offer banner is Relative. If it is, verify that the correct object ID is configured in the banner properties.
2. Check if the object configured in the offer is present on the web page where you are trying to display the offer.

Cause 7: Offers Displayed on Specific Browsers Only

When the same page is accessed from different browsers, offers are displayed on some browsers but not all.

**Recommended actions:**
1. Capture the HttpWatch or Fiddler traces on the browsers where offers are getting displayed and where they are not getting displayed. For details about these tools, see “Fiddler or HttpWatch” on page 40.
   - Capture the requests and responses from the working browser starting from when the web page is loaded till the offer is shown.
   - Capture the requests and responses from the problematic browser starting from when the web page is loaded till the time offer is expected to be shown.
2. Save the results and share them with the Cisco TAC team for further analysis.

Further Analysis

1. Run the following query on the active database to enable website debugging for offers:

   `UPDATE EGPL_CONFIG_PROPERTY SET VALUE = 'true' WHERE DOMAIN = 'egpl_general.properties' AND NAME = 'OFFERS_ENABLE_WEBSITE_DEBUG_INFO'`

2. From the Tools Console, clear the offers cache by using the **Clear Offers cache** utility.

3. Launch a web browser. Access the web page where offers are configured. A new debug window will open, which will capture debugging information for offers. Make sure that the pop-up blocker is turned-off on this browser.

4. Perform the actions which should trigger offers on the web page. This should log messages in the debug window. Capture the information from the window and contact Cisco TAC.

5. After the issue has been resolved, you must turn off the website debugging by running the following query on the active database:

   `UPDATE EGPL_CONFIG_PROPERTY SET VALUE = 'false' WHERE DOMAIN = 'egpl_general.properties' AND NAME = 'OFFERS_ENABLE_WEBSITE_DEBUG_INFO'`

6. From the Tools Console, clear the offers cache by using the **Clear Offers cache** utility.
Symptom 2: All Offers Configured for a Web Page Not Displayed

Multiple offers are configured for a web page, but the visitor is presented only one offer. After the first offer is presented, any of the subsequent offers are not presented even when the customer becomes eligible for those offers.

Cause: Web Page Configured to Display Only One offer

For the web page, the Stop after one offer is presented option is selected. As a result, only one offer is presented for that web page.

Recommended actions:

- From the Offers Console, change the Stop after one offer is presented setting for the web page where you want to display multiple offers.
Knowledge Base Issues

- Multiple Language Knowledge Base Issues
- Approval Process Issues
- Knowledge Workflow Issues
This chapter describes recommended actions for the most common issues related to the Knowledge Base.

Multiple Language Knowledge Base Issues

Symptom 1: Import Process of Language Files Fails

The following error occurs while importing translated content into the Knowledge Base:

Error Occurred.
Click the link below to open file from current server location or save it on your local machine.
Log file: eg_log_knowledge_import_1022.log

Cause: XML Format Changed in Translations Files

While translating the content in the XML file, if the user accidentally deletes some XML tags from the file, the import will fail.

Recommended actions:

- Check the contents of the XML file you are importing and make sure that the format of the file is intact.

Symptom 2: Attachments Not Displayed in All Languages

Article attachments are displayed with articles in one language, but not others.

Cause: Attachments Not Added to Articles in All Languages

When an attachment is added to an article and the same article is accessed in other languages, the attachment is not shown with the article. This is the designed behavior.

Recommended actions:

- To make attachments available with the article in other languages, you have to access the article in those languages and explicitly attach the files for each language.
Symptom 3: Changes Made to KB Objects Not Reflected in All Languages

Any changes made to KB folder names, article content, etc. are not reflected in all languages.

Cause: Updated Content Not Translated in All Languages

For the updated labels and content to display in other languages, the content from the source language must be translated to those languages.

Recommended actions:
- Check if the content has been translated in all languages.

Symptom 4: Export and Import Translations Buttons Not Available to Authors

Authors are not able to import translated content or export content for translations as the Export Translation and Import Translations buttons (part of the Import/Export button) are not available in the Knowledge Base Console toolbar.

Cause: Actions Not Assigned to Authors

The Import Translation and Export Translation actions are not part of the default Author role as the administrators may want to restrict the users who can perform these actions. Administrators have to explicitly assign these actions to authors.

Recommended actions:
- Login to the application as an administrator and assign the Import Translation and Export Translation actions to users who should be able to manage content for translations.

Symptom 5: Some Folders Missing From Translation File

The translation file does not contain all the folders selected for translation, or some of the sub-folders are missing from the file.

Cause: Sub-Folders Not Automatically Selected for Translation

When new folders are added under existing folders, they do not inherit the property set for the Translate content property. You have to configure this setting manually.

Recommended actions:
- From the Knowledge Base Console, check to make sure that the Translate content property is enabled for all the folders that you wish to translate.
Approval Process Issues

Symptom 1: Unable to Edit or Delete Approval Processes

An author trying to edit or delete an approval process receives an error message saying that the approval process is in use.

Cause 1: Configured Approval Process has Pending Articles

You cannot edit or delete an approval process if there are any articles in the scope of the process that are waiting to be approved, or have been sent back with feedback.

Recommended actions:
1. From the Knowledge Base Console, use the Search feature to look for articles that are waiting to be approved or have been sent back with feedback to the suggester.
2. If articles have been sent back with feedback to users, you would need to contact Cisco TAC to get the articles cleared from the system.
3. If there are articles sent back to agents with feedback, contact the agents to act on the articles so that the approval process can be completed for the articles. If you have large number of articles in this state and you need further assistance, contact Cisco TAC to get the articles cleared from the system.

Cause 2: Approval Process has Multiple Approval Levels

If the approval process has multiple approval levels, all the users in the process must approve the suggested article. If there is any article at any level pending approval, you will not be able to edit or delete the approval process.

Recommended actions:
1. Run the following query on the active database to find the ID of the department for which you want to edit or delete the approval process.
   
   select * from egpl_department

2. Run the following query to find the ID of the approval process.
   
   select * from EGPL_APPROVAL_PROCESS where DEPT_ID = Department_ID

3. Run the following query to find the list of articles waiting to be approved and the names of the users who need to approve them:
   
   select SUGGESTION_ID, USER_NAME, article_name from EGPL_PROCESS_SUGGESTION
   inner join egpl_user on egpl_user.user_id = EGPL_PROCESS_SUGGESTION.CURRENT_APPROVER
   inner join EGPL_KB_ARTICLE on EGPL_PROCESS_SUGGESTION.SUGGESTION_ID = EGPL_KB_ARTICLE.ARTICLE_ID
   inner join EGPL_KB_ARTICLE_VERSION on EGPL_KB_ARTICLE.ARTICLE_ID = EGPL_KB_ARTICLE_VERSION.ARTICLE_ID
4. **Contact the users to get the articles approved.**

**Symptom 2: Authors Unable to Approve Articles**

Authors see the articles waiting to be approved, but the **Accept**, **Reject**, and **Feedback** buttons are disabled and the authors cannot act on the suggestions.

**Cause 1: Manage Suggestions Permission Not Assigned on Folders**

Authors need to be assigned the “**Manage Suggestions**” permission on the KB folders to be able to work on the suggested articles.

**Recommended actions:**

- From the Administration Console or the Knowledge Base Console, check the user permissions and make sure that the “**Manage Suggestions**” permission is assigned to the authors on the KB folders where they need to work on suggestions.

**Cause 2: Approval Process has Multiple Approval Levels**

If the approval process has multiple levels, the suggestions have to be approved at the first level to be available at the next level.

**Recommended actions:**

1. From the Knowledge Base check if the approval process has multiple levels.
2. Run the following query on the active database to find the list of articles waiting to be approved and the names of the users who can approve them:
   ```sql
   select SUGGESTION_ID, USER_NAME, article_name
   from EGPL_PROCESS_SUGGESTION
   inner join egpl_user on egpl_user.user_id = EGPL_PROCESS_SUGGESTION.CURRENT_APPROVER
   inner join EGPL_KB_ARTICLE on EGPL_PROCESS_SUGGESTION.SUGGESTION_ID = EGPL_KB_ARTICLE.ARTICLE_ID
   inner join EGPL_KB_ARTICLE_VERSION on EGPL_KB_ARTICLE.ARTICLE_ID = EGPL_KB_ARTICLE_VERSION.ARTICLE_ID
   inner join EGPL_KB_ARTICLE_DATA on EGPL_KB_ARTICLE_DATA.ARTICLE_REFERENCE_ID = EGPL_KB_ARTICLE_VERSION.ARTICLE_REFERENCE_ID
   ```
Knowledge Workflow Issues

Symptom 1: Knowledge Workflows Option is Disabled for Authors

Authors are not able to create and manage knowledge workflows.

Cause: Knowledge Base Manager Role Not Assigned to Authors by Default

Only users with the Knowledge Base Manager role can configure knowledge workflows. The Knowledge Base Manager role must be explicitly assigned to the author by an administrator.

Recommended actions:

- From the Administration Console, assign the Knowledge Base Manager role to the author.

Symptom 2: Articles Not Displayed in My Work List After Sending to Review

Authors are not able to see their articles in their My Work list after the article has been sent for processing through a knowledge workflow, though the article is still visible in the parent folder.

Cause: Articles Under Review Considered Workable Only for Reviewers

The system considers an article sent out for review a workable item for reviewers, but not authors, and will not list the item in an author’s My Work list.

Recommended actions:

- No actions required.

Symptom 3: Reviewers Cannot See Articles in the KB Folder and My Work List

A knowledge workflow is configured and assigned reviewers by a knowledge base manager, but the reviewers are not able to see the articles from the KB folder and My Work list.
**Cause: View Permission For KB Folder Not Assigned to Reviewers**

Users must have view permission of a folder to see objects within. By extension, an article cannot be listed in the My Work list if the author cannot see the article. Permission to view the KB folder has not been assigned to article reviewers, preventing them from accessing articles within the KB folder.

**Recommended actions:**

- From the Administration Console, assign view permission for the KB folder to the reviewers.

**Symptom 4: Reviewer Cannot Check-Out Articles**

A knowledge workflow is configured and assigned reviewers by a knowledge base manager, but the reviewers are not able to check-out articles from the KB folder and My Work list.

**Cause: Edit Article Permission Not Assigned to Reviewers**

Permission to edit articles in the KB folder has not been assigned to article reviewers, preventing them from accessing articles within the KB folder.

**Recommended actions:**

- From the Administration Console, assign edit article permissions for the KB folder to all reviewers.
Archive Issues

- Overview
- Archive Jobs Issues
- Purge Jobs Issues
Overview

Data is stored in the active database. With time, the size of the data usually increases to a point where it begins to affect the performance of the system. 40 GB should be considered the maximum limit for the size of the active database, after which we recommend archiving to avoid performance issues. Hence, it is important that data which is not in use anymore is stored somewhere other than the active database.

Archiving is a systematic process which moves data from the active database to the archive database. Periodic archiving helps to keep the size of the active database within prescribed levels, thereby improving the performance of the system.

The list of tables that are archived are available in the `EGPL_CONFIG_PROPERTY` table in the active database. Run the following query on the active database to get this list:

```sql
SELECT * from EGPL_CONFIG_PROPERTY where DOMAIN = 'archive.egpl_arch_tablelist.properties'
```

To learn more about archiving, see the *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Administration Console*.

Archive Jobs Issues

Symptom 1: Scheduled Archive Jobs Do Not Run

The archive jobs do not run on schedule. This can happen for one of the following reasons.

Cause 1: Archive Service Not Running

The Archive service is not running. This service must be running for archiving to occur.

Recommended actions:

- From the System Console, check if the Archive service process and instance are running. If the service is not running, start the instance and process and see if this solves the problem.

Cause 2: Failed Jobs Exist in Application

There is a failed job in some department of the partition.

---

Important: The scenarios described in this chapter apply only to installations that use the Standard Edition of Microsoft SQL.
Recommended actions:

1. Check for failed jobs in all departments by running the following query on the active database:

   ```sql
   select a.job_name, b.department_name from egpl_arch_job a, egpl_department b
   where a.last_run_status = -1 and a.department_id = b.department_id
   ```

   If there are any failed jobs, the query will return the name of the job that has failed and the name of the department to which the job belongs.

2. From the Administration Console, navigate to the department and restart the failed jobs.

Cause 3: Stopped Jobs Exist in Department

There is a stopped job in the department.

Recommended actions:

1. Check for stopped jobs in all departments by running the following query on the active database:

   ```sql
   select c.job_name, b.department_name from egpl_arch_job_run a, egpl_department b, egpl_arch_job c
   where a.run_status = 2
   and a.department_id = b.department_id
   and a.job_id = c.job_id and a.department_id = c.department_id
   ```

   If there are any stopped jobs, the query will return the name of the job that is stopped and the name of the department to which the job belongs.

2. From the Administration Console, browse to the department and restart all stopped jobs.

Further Analysis

If none of the above mentioned recommended actions solve your problem, then collect the following data and send the information to Cisco TAC.

1. From the System Console, change the logging level for the archive process to `TRACE`.

2. Reproduce the problem again and collect the following data and log files.
   a. Send the following log files:
      * `eg_log_Server_Name_archive-process.log`
      * `egpl_root_Server_Name.log`
   b. Run the following query on the active database and send the results.
      ```sql
      > select job_id from egpl_arch_job with (nolock) where job_name like '
      'ArchiveJob%' and status=-1
      > select job_run_id from egpl_arch_job_run with (nolock) where
      job_id=<get the job_id from above query> and run_status=-1
      > select batch_id from egpl_arch_job_run_batch with (nolock) where
      ```
Symptom 2: Archive Jobs Fail

Archive jobs stop running and are shown in a failed state in the Administration Console.

To verify that failed jobs exist in the system, run the following query:

```sql
> select * from egpl_arch_batch_step with (nolock) where
batch_id=<batch_id from above query>
```

This could happen because of one of the following reasons.

### Cause 1: Database Users Do Not Have Correct Permissions

If the Cisco database users for the active database and reports database do not have DBO permissions on the databases, the archive jobs will fail.

**Recommended actions:**

1. Check the archive log file for errors. The following log message is recorded in the 
   $Cisco_Home\eService\logs\eg_log_Services_Server_Name_archive-process.log$ file when this 
   issue occurs.
   ```
   Login failed
   ```
2. Contact your database administrator and ask him to check if the Cisco database users for the active database 
   and reports database have DBO permissions on the databases.
3. If the permissions are not assigned, make the required changes.
4. From the System Console, restart the Archive service process.
5. From the Administration Console, restart the failed job and see if it runs successfully.

### Cause 2: Archive Database Unable to Connect to Active Database

The archive database is not able to connect to the active database, and as a result, the archive jobs are failing. 
This issue will be experienced only when the active database and the archive database are on different machines.

**Recommended actions:**

1. Check if the active database machine is able to connect to the archive database machine. You can check this 
   by doing the following:
   a. On active database server machine, open the Windows Command window.
   b. Type `telnet Archive database server machine 1433`. You should be able to connect to the archive 
      database. Port 1433 is the MS SQL server port on which you are connecting. For example, `telnet ArchiveDB 1433`. 

c. Similarly, run the command `telnet Active database server machine 1433` from the file server. For example, `telnet ActiveDB 1433`.

d. If you are not able to connect, there might be network connection problems. Contact your IT administrator to get the network problem fixed.

2. If network connection is fine, run the following query on the active database to check if the database link is working properly.

   ```sql
   SELECT * FROM [Archive.DB.Link.partition_ID]. egpl_casemgmt_case
   ```

   You can get the value for `Archive.DB.Link.partition_ID` from the active database by running the following query:

   ```sql
   SELECT * FROM EGPL_CONFIGPROPERTY WHERE DOMAIN = 'egpl_archiverconfig.properties' and NAME like 'archive.db.link.%'
   ```

3. If the link is broken, do the following:

   a. Connect to the active database server with a user who has administrator credentials.
   
   b. In the SQL Server Enterprise Manager, browse to `Server Objects > Linked Server > Archive Database Link` using the value you received in Step 2 from the `egpl_archiverconfig.properties` file.
   
   c. Right-click the link and select `Properties > Security`.
   
   d. In the window that opens, check the following:

      - **Local login**: This should be the user name of the active database user.
      - **Remote login**: This should be the user name of the archive database user.
      - **Remote password**: This should be the password of the archive database user.

   e. Correct the credentials, if they are incorrect. The database user names and passwords should be the same as provided at the time of installation of Cisco Unified EIM & WIM.
   
   f. Next, right-click the `Archive Database Link` and select `Server Options`.
   
   g. In the window that opens, check the following:

      - **Collation Compatible**: This should be set to `false`.
      - **Data Access, RPC, RPC Out, User Remote Collation**: These should be set to `true`.
      - **Collation Name**: This property should be blank.
      - **Connection Timeout, Query Timeout**: These should be set to 0 (zero).

   h. After making these changes, run the following query again to check if the link is working now.

   ```sql
   SELECT * FROM [Archive.DB.Link.partition_ID]. egpl_casemgmt_case
   ```

4. From the System Console, restart the Archive service process.

5. From the Administration Console, restart the failed job and see if it runs successfully.

---

**Cause 3: Archive Service Not Restarted After Adding Custom Attributes**

All archive jobs in the application start failing. This issue is observed because archive jobs are not restarted after adding custom attributes from the Tools Console. When a custom attribute is added, the active database changes, but the archive database is not updated with the latest attribute information. To update the archive database, the
Archive service process and instance needs to be restarted. If you do not do that, the archive jobs will keep failing.

**Recommended actions:**

1. Check the archive log file for errors. The following log message is recorded in the `Cisco_Home\eService\logs\eg_log_Services_Server_Name_archive-process.log` file when this issue occurs.

   
   column mismatch or too many columns or columns <column> not present in ArchiveDB table

2. From the System Console, restart the Archive service process and instance.

3. From the Administration Console, restart the failed archive job and see if it runs successfully.

**Cause 4: Transaction Logs are Full**

If the transaction logs for the archive database is full, archive jobs will not run.

**Recommended actions:**

1. Check the archive log file for errors. The following log message is recorded in the `Cisco_Home\eService\logs\eg_log_Services_Server_Name_archive-process.log` file when this issue occurs.

   The transaction log for database <ArchiveDB> is full.

2. Contact your database administrator and ask him to check if the transaction logs file is full. If that is the case, the Database Administrators will need to increase the size allocated for this file. The database administrator can also choose to shrink the transaction logs file on regular basis. For details about performing these tasks, you can also look at the Microsoft documentation.

3. From the System Console, restart the Archive service process and instance.

4. From the Administration Console, restart the failed archive job and see if it runs successfully.

**Cause 5: Archive Database is Full**

If the archive database is full, archive jobs will not run.

**Recommended actions:**

1. Check the archive log file for errors related to database size `Cisco_Home\eService\logs\eg_log_Services_Server_Name_archive-process.log`.

2. Contact your database administrator to check if the archive database is full. If this is the problem, purge the data by running the Purge job from the Administration Console. If you cannot run the Purge job, consider increasing the size allocated to the database.

3. Contact your database administrator to check if the disk on which you have stored the archived data files is full. If this is the problem, increase the disk space.

4. From the System Console, restart the Archive service process and instance.

5. From the Administration Console, restart the failed archive job and see if it runs successfully.
Further Analysis

If none of the above mentioned recommended actions solve your problem, then you need to collect additional data and send the information to Cisco TAC. For details, see “Further Analysis” on page 149.

Purge Jobs Issues

Symptom 1: Purge Jobs Do Not Run

The Purge jobs do not run on schedule.

To validate this, check the purge schedule time. Look for the settings `purge.start.time.1` and `purge.end.time.1` in the active database in the `EGPL_CONFIG_PROPERTY` table by running the following query:

```
Select * from EGPL_CONFIG_PROPERTY where domain = 'egpl_archiverconfig.properties'
and NAME like 'purge%'
```

If the current time of the services server is within the purge’s scheduled time, then the Purge job should run. Situations where it does not run may occur because of one of the following reasons:

Cause 1: Archive Service Not Running

The Archive service is not running. This service is required to be running for a purge to happen.

**Recommended actions:**

- From the System Console, check if the Archive service process and instance is running. If the service is not running, start the instance and process and see if this solves the problem.

Cause 2: Failed Purge Jobs Exist in Application

There is a failed job in some department in the partition.

**Recommended actions:**

1. Check for failed jobs in all departments by running the following query on the active database:

   ```
   select c.job_name, b.department_name from egpl_arch_job_run a, egpl_department b, egpl_arch_job c
   where a.run_status = -11
   and a.department_id = b.department_id
   and a.job_id = c.job_id and a.department_id = c.department_id
   ```

   If there are any failed jobs, the query will return the name of the job that has failed and the name of the department to which the job belongs.

2. From the Administration Console, browse to the department and restart the failed purge job.
Further Analysis

If none of the above mentioned recommended actions solve your problem, then you need to collect additional data and send the information to Cisco TAC. For details, see “Further Analysis” on page 149.
Reports Issues

- Overview
- Setup and Performance Issues
- Report Run and Schedule Issues
- Report Results Issues
Overview

A report contains historical data, recorded by the system and built from summarization jobs, about a particular facet of your service organization.

Reports are created from templates—all templates are available in the Reports Console, and three of them are also available in the Agent Console.

Customers who are using Microsoft SQL Enterprise version have a separate reports database. The separate reports database can be on the same server as the active database or on a different machine. Separating the reports database helps to speed up interactive application performance by removing resource-intensive report summarization and report generation tasks from the active database.

To learn more about reports, see the Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Reports Console.

Setup and Performance Issues

Symptom 1: Unable to Run Reports

On running a report, the ‘Generating…’ screen is displayed indefinitely.

Cause: Out of Memory Error Causes Reports Service to Fail

This issue is observed when the Reports service fails because of an out of memory error.

Recommended actions:

1. In the following log files, search for “OutOfMemory”. If the error is present, you need to increase the Java Virtual Machine (JVM) size for the Report service process.
   - Cisco_Home\eService\logs\eg_log_Services_Server_Name_report-process.log
   - Cisco_Home\eService\logs\eg_log_Application_Server_Name_ApplicationServer.log

2. Run the following query on the active database:

   Insert into egpl_config_property values ('egpl_dsm.xml', 'JVMParams.Process-Name',' -Xmx512m', null)

3. Search for </JVMParams> and after it, add the following:

   <JVMParams>
     <default>-Xmx128m</default>
     <Report_Process_Name>-256m</Report_Process_Name>
   </JVMParams>

   Where Report_Process_Name is the name of the report process for which you want to increase the JVM size. To get the name of the report process, log in to the System Partition and go to System Console. Navigate to
the folder **System > Shared Resources > Services > General > Report**. Select the folder **Report** to view the details, including the name, of all the report processes in the List pane.

4. Restart the application.

**Symptom 2: Data Not Moved from Active Database to Reports Database**

Transfer of base data from the active database to the reports database does not occur, or is not synchronized with the latest date and time. This issue is specific to customers using a SQL Enterprise version.

**Cause: Specific Problems With Copying Reports Data**

Some problems that can occur are:

- Populate summary jobs are not scheduled for execution, or the jobs are not active.
- Execution of a Reports job failed with a SQL error e.g. Primary Key (PK) violation etc.
- Reports job runs successfully, but skips a few rows in some of the tables.

**Recommended actions:**

1. Run the following query on the reports database to check if the summarization jobs ran successfully.

   ```
   select * from egplr_scheduled_task_status
   ```

2. Check if there are any errors in the **EGMNT_ERRORS** table on the reports database. The stored procedure (SP) `usp_plr_mnt_data_move` is executed after every 30 minutes as part of the SQL job on the active database to move data from certain tables to the reports database. If any of the steps fail, it logs the error in the **EGMNT_ERRORS** table with details such as the error number, error message, table name, version, and create date of the table row.

3. Check the history of the populate job on the reports database and see if there is any failure for the step:

   ```
   mnt_data_move_populatesmy_<<eGReportsDB>>
   ```

4. Validate counts for data in the active database and match with replicated counts on the reports database. Open the SP `usp_plr_mnt_data_move` of the reports database and see the tables involved for which insert statements are present in that SP. Check if counts are matching for these tables in the active database and the reports database.
Report Run and Schedule Issues

Symptom 1: Reports Notifications Not Sent Out

Email notifications for reports are not sent out to the users.

Cause: Invalid SMTP Server Settings

SMTP Server settings have not yet been configured, or have not been configured correctly. Email notifications for reports cannot be sent out to users while the server settings are not configured properly.

Recommended actions:

1. From the Reports Console check if the correct email addresses are provided for the notifications.
2. From the Administration Console check if the value of the partition level setting Notification mails SMTP Server is configured correctly.

Symptom 2: “Report Service Not Running” Error While Running Reports

While running reports, the user sees a Report service not running error.

Cause: Report Service Not Running

The Report service is stopped or has not been started. Reports cannot be generated while the Report service is stopped.

Recommended actions:

- In the system partition, access the System Console and start the Report service.

Symptom 3: “No Data Found” Message

When a user runs a report, the report results display a No data found error or all columns are populated with zeros.

Cause: Summarization Job Not Completed for Specified Date

This occurs when summarization for that report has not been completed up to the date for which the report is run.

Recommended actions:

1. Check the status of populate jobs on the active database or reports database (whichever applies) and confirm that all the steps are in a completed state i.e., ‘Done’. Then, check the job history and see if any errors have occurred.
2. Check the status and lastrun_datetime for each script in the egplr_scheduled_task_status table on the active database or reports database. The status should be done and the lastrun_datetime should be close to the current date and time with the maximum lag of half hour. (101 script would be always behind by 7 days). The report SP ( Stored Procedure) and the output table can be obtained from the EGPL_RPT_TEMPLATES table available in the Cisco Unified EIM & WIM active database.

3. Check for any error logged in the EGPL_RPT_JOB_ERRORLOG table in the active database or reports database by the stored procedure executed as part of the job.

4. If your deployment has a separate reports database, check if the synchronization of event data has been completed to the latest time. Data copying is always run before populating SPs. See, “Symptom 2: Data Not Moved from Active Database to Reports Database” on page 157.

Symptom 4: Error While Viewing Report Results

When a user runs a report, the report result window shows the message:

An error occurred while running this report.

Report generation is a two step process:

1. The reports SP ( Stored Procedure) runs and loads the data in the output table. There may be some SQL errors while this SP is executed. Failure can occur when the reports SP takes longer than the configured time (default 10 minutes) to execute, canceling the SP.

2. The second stage is the generation of the output file (.jprint) by the Reports service and population of the reports UI page with the data from the output table. This is done with the help of Jasper ( third party tool).

Recommended actions:

1. Check the disk space available on the file server. Because of disk space issues, the Reports service may not have been able to generate output file in the Cisco_Home\eService\reports\1\history\report_template_id folder.

2. Check the following log files for reports related errors:
   - eg_log_Server_Name_report-process.log
   - eg_log_Server_Name_ApplicationServer.log
   - egpl_root_Server_Name.log

3. Look for the “Failed to LOAD…” error message in the reports log file. The cause of stored procedure failure is logged along with the error. It is also logged in the EGPL_RPT_ERRORLOG table. This error can occur because of two reasons:
   a. SQL error occurs during SP execution. Debug the stored procedure.
   b. If the logs show the following error for that report ID, then the SP execution was terminated because it was taking a long time to execute.

   Failed to LOAD data for Report Generation Task with Report Id:12339 & Run Id:20627. <@> [Microsoft][SQLServer 2000 Driver for JDBC ] The operation was cancelled at the user's request.

4. Look for “Failed to FILL…” text in the reports log file. Check if that message always occurs when that report is run. If yes, then the Jasper files need to be debugged. Contact Cisco TAC for help with debugging this issue.
5. Look for “Failed to LOAD...” error messages in the reports log file. The reason the stored procedure failed and displayed this error message is recorded in the log file and in the EGPL_RPT_ERRORLOG table. The “Failed to load” error generally occurs when a SQL error is encountered while executing the reports SP. Contact Cisco TAC for help with debugging this issue.

Report Results Issues

Symptom: Mismatch in Reports Data

The Reports count does not match with the real time data/monitors based on some user analysis for some specific columns. The Reports count should not be compared with real time data/monitor counts as reports always show historical data with a lag time of at least half an hour, due to the summarization process schedule. Most of the time, a comparison of reports counts with real time data is not a valid comparison.

Incorrect counts may also be displayed if certain events were missing due to manual updates being made to tables in the DB, e.g. changes to the state of activities.

Recommended actions:

1. Review the Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Reports Console with the customer to clarify the discrepancy on definitions for the columns.

2. Contact Cisco TAC for help with debugging this issue.
Database Issues

- Overview
- Database Slowness Issues
Overview

This chapter outlines common issues in the application’s databases. The impact of these issues is usually felt in the overall performance of the system.

Database Slowness Issues

Symptom: Application Slows Down

Cause 1: Inadequate Disk Space

Inadequate disk space on the database server can cause the application to slow down. As a general guideline, there should be at least 100 GB of free space.

Recommended actions:

1. Check the disk space available on the drive where the MSSQL database is installed. Make sure that there is at least 100 GB of free space.

2. If there is not enough disk space, shrink the database to release the more space.
   Run the following query to shrink the SQL server tempdb, and the Unified EIM and WIM active, master, archive, and reports databases.
   ```sql
   use Database_Name
   go
   dbcc shrinkdatabase(n'Database_Name')
   go
   ```

3. If the required disk space is not freed by this process, consider upgrading the hard disk.

Cause 2: Antivirus Running on Database Server

The application will slow down if the antivirus runs during peak hours. 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.

Recommended actions:

- For details of the files and folders that you need to exclude from the virus scanner, see the “Configuring Virus Scanning Exclusions” section in the Cisco Unified Web and E-Mail Interaction Manager Installation Guide.
Cause 3: Other Applications on the Database Machine Using Disk Space

Ensure that the database server resources are available exclusively for the Unified EIM and WIM application.

Recommended actions:
  - Uninstall or move the applications that are sharing the resources to free disk space.

Cause 4: Transaction Logs are Full

Transaction log file settings are not set to auto growth and thus, a few large SQL operations fill the transaction file. As a result, SQL cannot write any more transactions.

Recommended actions:
1. Run the following query on the Unified EIM and WIM active, master, reports, and archive databases to get the log file names and the size of the log files.

   ```sql
   SELECT name, max_size
   FROM sys.database_files
   WHERE type_desc LIKE '%LOG%'
   ```

   If the `max_size` of the log file is -1 or 268435456 (2 terabytes), then you do not need to change the maximum log file size.

2. To change the maximum size of the log file to unlimited, run the following query:

   ```sql
   USE [master]
   GO
   ALTER DATABASE [DATABASE_NAME] MODIFY FILE (NAME = N'LOG_FILE_NAME', MAXSIZE = UNLIMITED)
   GO
   ```

3. Run the following query to shrink the transaction log file. The size of the log file will be reset to 5 MB.

   ```sql
   USE [DATABASE_NAME]
   GO
   DBCC SHRINKFILE (N'LOG_FILE_NAME', 5)
   GO
   ```

4. You should also schedule a SQL maintenance job to backup the transaction log file at regular intervals.

Cause 5: Database Queries Taking Long Time to Run

If some queries take too long to run, it will slow the database.

Recommended actions:
1. Access the query timeout log file from the location

   ```
   Cisco_Home\eService\logs\log_log_query_timeout.log
   ```

   on the file server and look for queries that are taking a long time to run and the frequency of these occurrences.
a. Search for the text “Time taken by Query (ms)” in the log file. This tells how many milliseconds the query took to execute.

b. Look for the query name “Query Name:” and the Query text “Query Text:” corresponding to the queries that are taking a long time to run.

2. Validate if the hardware configuration meets the numbers recommended in the Cisco Unified Web and E-Mail Interaction Manager Solution Reference Network Design Guide.

3. Do the following to check if the SQL server is configured properly.

a. Run the following query to check if the MSSQL edition is correct.

```sql
SELECT @version
```

b. Run the following queries to find out the minimum and maximum memory allocated to the MS SQL database.

```sql
EXEC sys.sp_configure N'min server memory (MB)'
EXEC sys.sp_configure N'max server memory (MB)'
```

If the values do not match the numbers recommended in the Cisco Unified Web and E-Mail Interaction Manager Solution Reference Network Design Guide, run the following queries to change the numbers.

```sql
EXEC sys.sp_configure n'max server memory (mb)', n'Maximum_Size'
go
reconfigure with override
go
```

c. Check the database properties. Select the database, right-click and select Options and make sure Auto Update Statistics is set to True.

4. Run the following query to check if Snapshot Isolation is enabled.

```sql
SELECT name, is_read_committed_snapshot_on FROM sys.databases WHERE name = 'Database_Name'
```

The value 0 in the is_read_committed_snapshot column indicates that Snapshot Isolation is disabled. The value 1 indicates that it is enabled.

If the Snapshot Isolation is disabled, run the following query to enable it.

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

5. Run the following query to find out the queries that are blocked:

```sql
SELECT * FROM sys.sysprocesses
WHERE blocked <> 0
```

From the output of this query, get the SPID of the blocked process to find out the actual query causing the block. Run the following query using the SPID.
DBCC inputbuffer (SPID)

The EventInfo column of the query results will display the query that is blocked. Provide this information to Cisco TAC for further analysis.

6. Collect the SQL profiler trace information and provide this information to Cisco TAC for further analysis. Do the following:
   a. Open the SQL profiler from Start > All Programs > Microsoft SQL Server 2012 > Performance Tools > SQL Server Profile.
   b. Using the File > Template > Import Template menu option, import the template file provided to you by Cisco TAC.
   c. Run the trace by creating a new trace file and select the template, and save the trace file.

7. Enable deadlock traces to identify which queries are causing deadlocks. Do the following:
   a. Run the following query to enable deadlock traces:
      \[\text{dbcc traceon (1222,1204,-1)}\]
   b. Run the following query to verify that the dbcc tracing is turned on from the query analyzer:
      \[\text{dbcc tracestatus (-1)}\]
      The error log file will be generated at the following location MSSQL_Home\MSSQL\LOG. This file has all the queries that are blocking and causing the deadlock. Send this file to Cisco TAC for further analysis.
   c. Search the log files in the Cisco_Home\eService\logs folder for the term deadlock. If you find that such log messages exist, share the log files with Cisco TAC.

8. Use the Windows Performance Monitor Tool and capture the performance counters for the following parameters. Save the output to a file and send it to Cisco TAC.
   - SQLServer:Buffer Manager > Buffer cache hit ratio
   - SQLServer:General Statistics > User Connections
   - SQLServer:Locks(_Total) > Number of Deadlocks/sec
   - SQLServer:Memory Manager > Connection Memory (KB)
   - SQLServer:Memory Manager > Target Server Memory (KB)
   - SQLServer:Memory Manager > Total Server Memory (KB)
   - System > Processor Queue Length
   - Memory > % Committed Bytes In Use
   - Memory > Available MBytes
   - Memory> Pages/sec
   - PhysicalDisk\% Idle Time
   - PhysicalDisk(_Total) > Avg. Disk Queue Length
   - PhysicalDisk(_Total) > Avg. Disk sec/Read
   - PhysicalDisk(_Total) > Avg. Disk sec/Write
   - Processor(_Total) > % Processor Time
   - Process(sqlservr) > Private Bytes