



Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to System Console

For Unified Contact Center Enterprise and Hosted and Unified ICM

Release 4.3(1)

October 2009

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to System Console: For Unified Contact Center Enterprise and Hosted and Unified ICM
© 2009 Cisco Systems, Inc. All rights reserved.

Contents

- Preface6**
 - About This Guide 7
 - Document Conventions..... 7
 - Other Learning Resources..... 8
 - Online Help 8
 - Document Set 8

- Chapter 1: Console Basics10**
 - Key Terms and Concepts 11
 - Elements of the User Interface 13

- Chapter 2: Setting up the System.....15**
 - Role of a System Administrator 16
 - Identifying Requirements 16
 - Managing Resources 16
 - Across the System 16
 - Within the Business Partition 17
 - Setting up Services 17
 - Setting up Unified EIM Services 17
 - Setting up Unified WIM Services 25
 - Setting up Standalone Email Services..... 27
 - Setting up Standalone Chat Services..... 27

- Chapter 3: Business Partition.....28**
 - About the Business Partition..... 29
 - Managing the Business Partition..... 29
 - Managing Service Instances 29
 - Increasing the Number of Service Instances 29
 - Removing Service Instances 30
 - Viewing Database Details 31

| | |
|--|----|
| Configuring Database Details | 32 |
| Assigning Permissions | 33 |

Chapter 4: Managing Hosts34

| | |
|--------------------------|----|
| About Hosts. | 35 |
| Editing Hosts. | 35 |
| Deleting Hosts. | 36 |
| Stopping Hosts | 36 |
| Starting Hosts | 36 |

Chapter 5: Services37

| | |
|---|----|
| About Services, Service Processes, and Service Instances | 38 |
| Services | 38 |
| Chat Service. | 39 |
| Content Index Services | 39 |
| External Agent Assignment Services | 39 |
| Email Services | 39 |
| General Services | 39 |
| Knowledge Base (KB) Services | 40 |
| Listener Services | 40 |
| Workflow Services | 40 |
| Service Processes | 41 |
| Service Instances | 41 |
| Managing Service Processes | 41 |
| Creating Service Processes | 41 |
| Deleting Service Processes | 42 |
| Increasing the Number of Instances for Service Processes. | 42 |
| Starting Service Processes. | 43 |
| Stopping Service Processes. | 43 |
| Managing Service Instances | 44 |
| Creating Service Instances | 44 |
| Deleting Service Instances | 45 |
| Starting Service Instances | 45 |
| Stopping Service Instances | 46 |
| Adding Aliases to Retriever Instances | 46 |
| Configuring the MR Connection Port for an EAAS Service Instance | 46 |
| Configuring a Listener Service Instance | 47 |

Chapter 6: Loggers and Appenders48

- About Loggers and Appenders 49
 - Loggers 49
 - List of Loggers Available in the System..... 49
 - Appenders 49
 - List of Appenders Available in the System..... 50
- Managing Loggers 52
 - Viewing Loggers 52
 - Changing the Trace Level of Loggers..... 52
- Managing Appenders 53
 - Viewing Appenders..... 53
 - Changing the Trace Level of Appenders..... 54

Chapter 7: Monitors.....55

- About Monitors 56
 - Host Monitors 56
 - Service Process Monitors 57
 - Service Instance Monitors..... 57
- Configuring Monitors 58
- Deleting Monitors 60
- Starting Monitors 60

Preface

- ▶ [About This Guide](#)
- ▶ [Document Conventions](#)
- ▶ [Other Learning Resources](#)

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

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

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

About This Guide

Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to System Console introduces you to the System Console and helps you understand how to use it to set up and monitor system services.

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

Document Conventions

This guide uses the following typographical conventions.

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


Document conventions

Other Learning Resources

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

Online Help

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

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

Online help options

Document Set

Unified WIM and Unified EIM 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/voicew/tsd_products_support_category_home.html

The document set contains the following guides:

- ▶ *Cisco Unified Web and E-Mail Interaction Manager Hardware and System Software Specification*
- ▶ *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*

1

Console Basics

- ▶ [Key Terms and Concepts](#)
- ▶ [Elements of the User Interface](#)

A highly specialized workspace for system administrators, the System Console helps you set up and manage the system resources needed for your system to function effectively.

At the highest level, the application has two distinct spaces. The system level space that deals with all those components that are relevant to the application as a whole, but do not have any direct relationship with the every day, business end of the application and the production level space that deals with the business end of the application. Architecturally too, the application is organized as two entities, with two databases, the master and the active and two different URLs - a system URL and a partition URL - to access the information within.

A single product installation may span multiple machines and databases. The unified view of System Console provides you with information about the system processes, machine load, and database servers.

Key Terms and Concepts

Partition

The installation program creates two distinct spaces: a system level space and a business partition. All components that are relevant to everyday production reside in the business partition and are stored in the active database. System level components and information relating to them; such as configuration details for System processes, system wide monitors etc., reside in the system level partition and are stored in the master database or in configuration files. The system-level space also provides the context for system administrators to administer components that affect the business partition, but are not directly related to the everyday use of the application.

Within Unified CCE, the term partition is used to refer to the business partition.

System administrator

System administrators perform technical administration functions to manage the system. Using the tools provided to them, they can monitor the status of the application, modify resource allocation and manage the servers on which the application components are installed. The installation program creates the first system administrator during the installation process. A user name and password is specified during installation and the program uses it to create a system administrator. Once the installation is complete, this user name can be used to log in to the application and create additional peer system administrators.

System administrator view

A system administrator has a holistic view of the System Console through a unique URL. This URL is typically used only by system administrators. Within the System Console there are two nodes at the highest level: Shared Resources and Partition. Some of the components a system administrator can view and administer within the Shared Resources node are:

- ▶ **Hosts:** servers that are part of the installation.
- ▶ **Logger:** loggers and logger appenders within the application.
- ▶ **Monitors:** custom monitors that keep you updated about the status of hosts and service processes.
- ▶ **Services:** processes used to perform various functions within the system E.g. retriever, dispatcher etc.

The system administrator can also view all the business partition specific monitors and service instances from within the Partition node.

Partition administrator

Partition administrators are users whose main focus is to create and maintain the components of the business partition. They create new departments and all the users within a department. Department level users can then log in to the system and set it up based on their business needs. Partition administrators have jurisdiction across departments. They have the ability to set up permissions that are shared across departments to enable users from one department to work with another department.

The first partition administrator is created by the installation program based on the user ID and password specified as part of the installation process. This partition administrator can then log in and create additional peer partition administrators using the user creation screens in the application.

Partition administrator view

A partition administrator has a partial view of the System Console from the partition URL. The tree displays only the Partition nodes and sub-nodes within it. The Shared Resources node is not visible to the partition administrator.

Shared resources

System administrators work with shared resources to enable hosts, services and service processes.

Partition resources

These are specific to the business partition. They consist of logs, monitors, and service instances. Typically, a partition administrator works with the partition resources.

Service processes

Services, through service processes, perform specialized functions within the system. These include, but are not limited to fetching and dispatching emails, routing activities through appropriate workflows and determining the appropriate agents for activity assignment. Service processes have to be started in order to enable the basic functioning of the system.

Service instances

Service instances are derivatives of service processes. Service instances are configured within the business partition to accomplish specific functions. These instances are specific to the business partition. Depending on the estimated workload, multiple instances of certain services can be created to improve the performance of the system.

Hosts

Hosts are the physical machines on which the application is installed and are configured from the System Console for the whole system.

Loggers

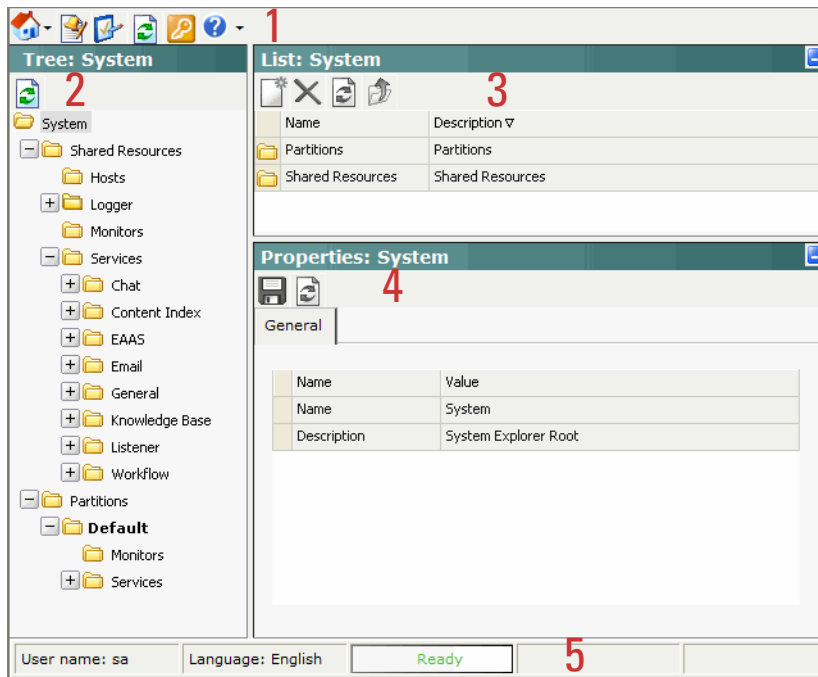
Loggers are used for maintaining and debugging applications. Developers embed various types of trace messages in the code at critical points. These trace messages are logged in appropriate files on client side or server side as per the settings, helping the maintenance engineers trace the cause of a problem.

Monitors

Monitors enable administrators to keep account of the status of operations. Different actions can be monitored from the System Console at shared resource level as well as the business partition level. Monitors can be set such that only required attributes are displayed in results.

Elements of the User Interface

The console user interface can be divided into five functional areas:



Elements of the console user interface

- 1. Console toolbar:** The main toolbar of the console appears at the top of the screen. It allows you to access some frequent commands with a single click.
- 2. Tree pane:** The Tree pane is your main navigation area. It displays the System tree with the main nodes (folders), Shared Resources and Partitions. Shared Resources and Partitions are further divided into the respective sub-branches such as Monitors and Services.

To expand all first and second level nodes with a single click, shift + click the plus [+] button next to the topmost node. The contents of all first and second level nodes are displayed in the Tree pane.
- 3. List pane:** The List pane displays first-level contents of the folder selected in the Tree pane. You can view the name, description, date of creation, etc., of the displayed items. Note that you can view only those columns that the administrator has permitted for display. In this pane, you can create items or select existing ones to modify or delete them.
- 4. Properties pane:** The Properties pane displays the contents of the item selected in the List pane. In this pane, you can edit the properties of the selected item.
- 5. Status bar:** The status bar is present at the bottom of every screen. It displays the following information:

- The user name with which the user has logged in the system.
- The language currently in use.
- The status of the system (**Loading**, **Ready**, etcetera).

Setting up the System

- ▶ [Role of a System Administrator](#)
- ▶ [Identifying Requirements](#)
- ▶ [Managing Resources](#)
- ▶ [Setting up Services](#)

Role of a System Administrator

As a system administrator you perform technical administration functions to manage the system. You can allocate and manage resources across different components of your system.

The installation program creates the first system administrator by prompting for the user name and password during installation. Use this account to log in to the System Console to manage system resources. You can also create additional system administrators.



Note: System administrators are not mapped to any Unified CCE users.

Identifying Requirements

Once the installation is complete, it becomes your primary responsibility, as a system administrator, to set up the system in an effective manner for your business needs. We recommend that you plan your requirements before configuring the system accordingly. This would typically include:

- ▶ Creating hosts and service processes
- ▶ Creating service instances within the business partition
- ▶ Configuring monitors to cater to different requirements

There could be many more such requirements that you need to plan out before actually setting about configuring your system.

Managing Resources

Across the System

System administrators have jurisdiction over the resources available at the system level. Shared resources help you enable services, processes, and hosts. The following folders are available within shared resources:

- ▶ **Hosts:** Configure hosts and their properties from the shared resources folder. Hosts are available throughout the system. However, you can create hosts only during installation.
- ▶ **Loggers:** You can view loggers, including appenders, from shared resources. The information required for inspection of the system is logged here.
- ▶ **Monitors:** Create and configure monitors to keep a check on the overall resource utilization. You can thus monitor the complete system and all its components.
- ▶ **Services:** Service processes are created from this node.

Within the Business Partition

System administrators as well as partition administrators work with partition resources to enable services, instances, and monitors specific to the business partition.

At the outset, the installation program creates the business partition. The modifications you make under partition resources node are applicable only to the business partition.

The following folders are available under the business partition:

- ▶ **Monitors:** Create and configure monitors to keep a check on partition resource utilization. You can monitor specific process instances as well.
- ▶ **Service Instances:** The service instances created from this node run for the business partition.

Setting up Services

Service processes are managed at the system level as shared resources. Service instances are managed within the business partition. See [“Managing Service Processes” on page 41](#) and [“Managing Service Instances” on page 44](#) for details of the procedures mentioned in this section.

Setting up Unified EIM Services

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

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

To set up Unified EIM services:

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



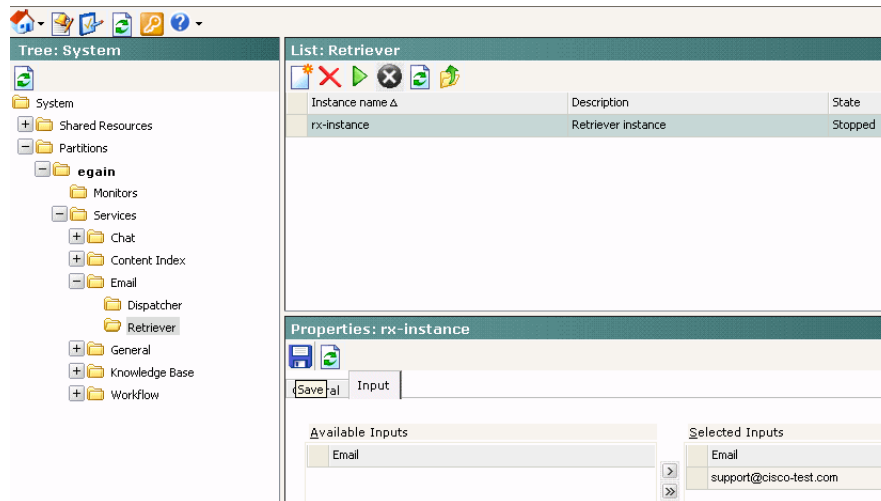
Log in as system administrator into system area

2. Go to the System Console.



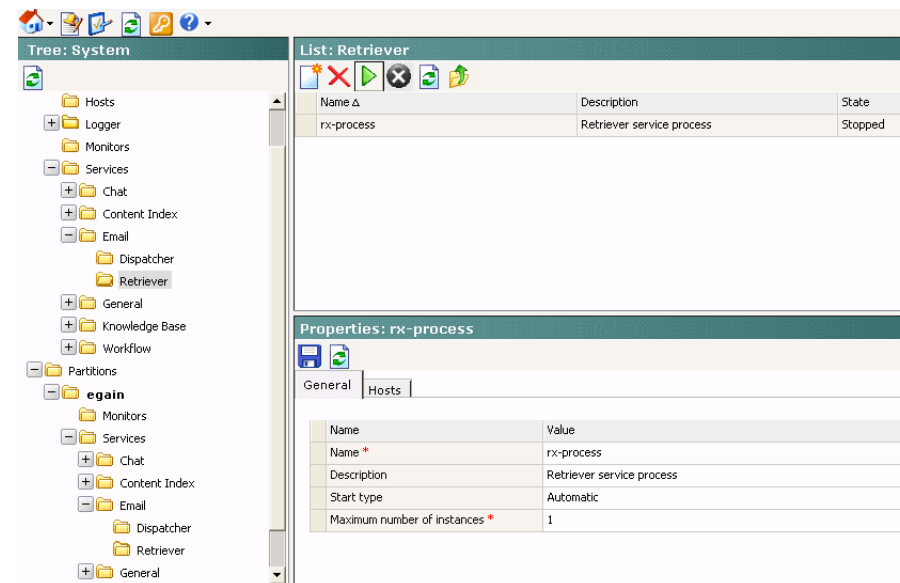
Select the System Console

- Browse to the **Partitions** > *Partition_Name* > **Services** > **Retriever** node. Click the Retriever instance you want to use, and select an available email alias.



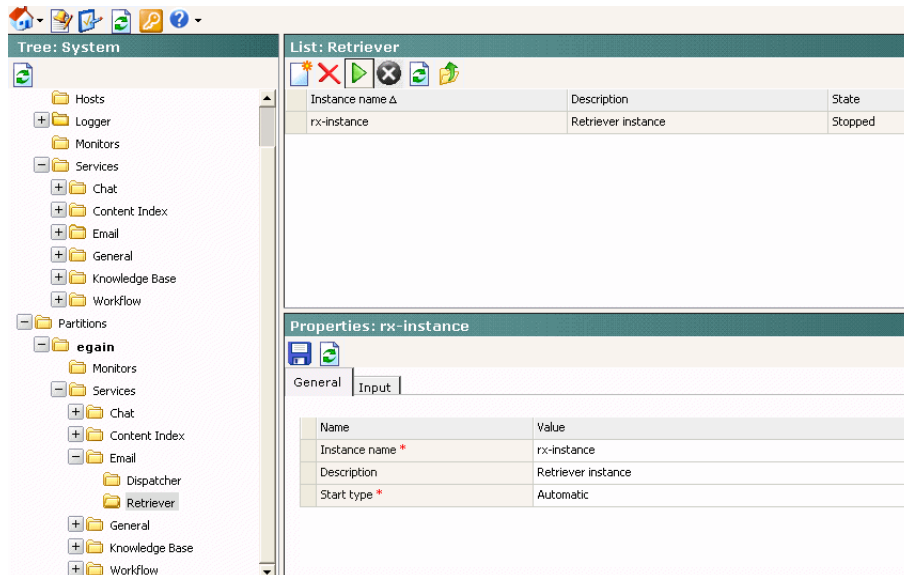
Associate a Retriever instance with the email alias created earlier

- Restart the Retriever process and instance based on the notification message that appears. Browse to **Shared Resource** > **Services** > **Retriever**, and stop and start the Retriever process for the system. Also ensure that the start type for the service process is set to automatic.



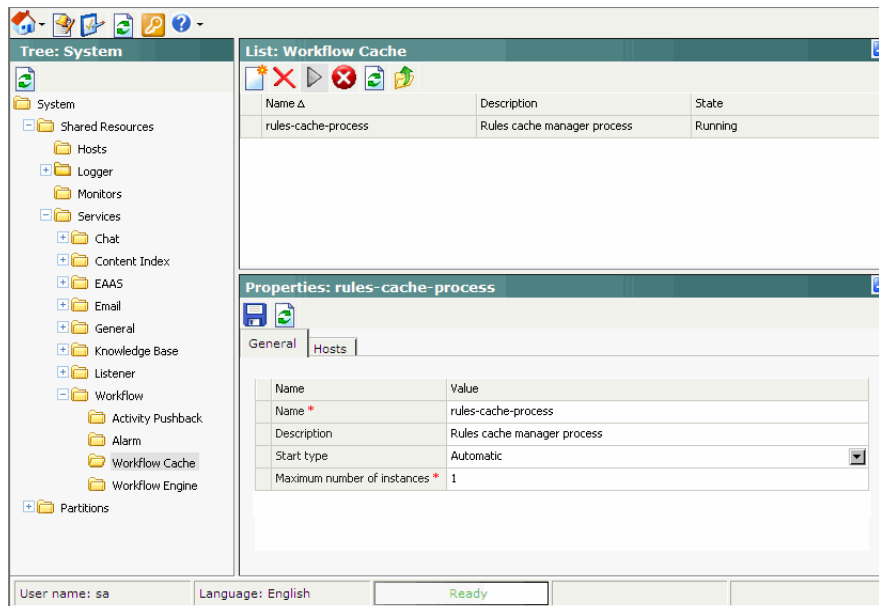
Start the Retriever process

5. Navigate back to the **Partitions** > *Partition_Name* > **Services** > **Retriever** node. Ensure that the start type for the service instance is set to automatic. Stop and start the Retriever instance.



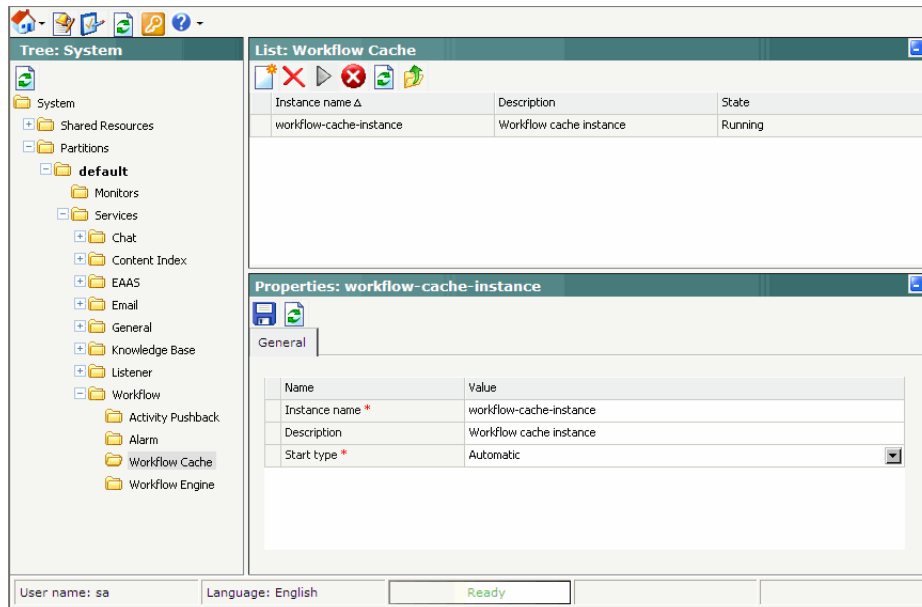
Start the Retriever instance

6. Browse to **Shared Resource** > **Services** > **Workflow** > **Workflow Cache** and verify that the Workflow Cache process is running. If the process is in a stopped state, start the process by clicking the **Run** button. Also ensure that the start type for the service process is set to automatic.



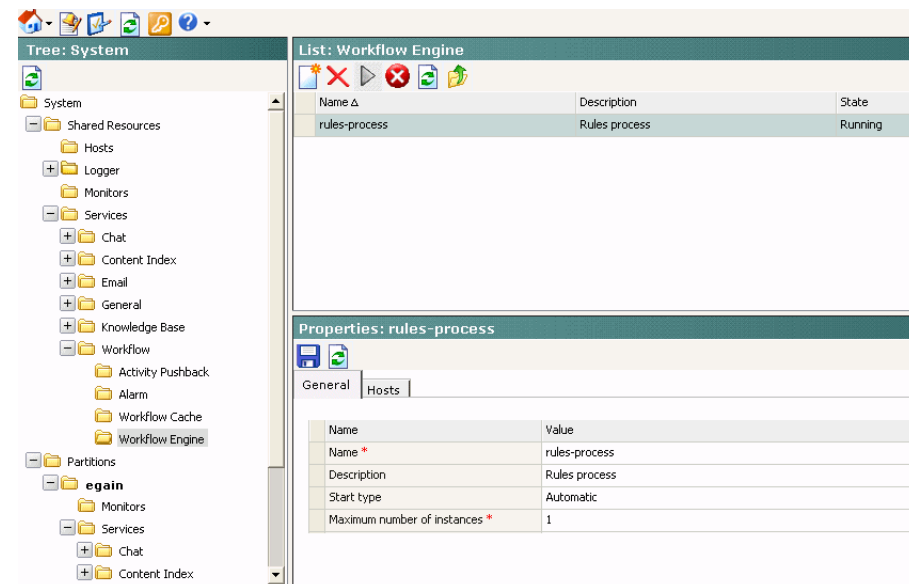
Start the workflow cache process

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



Start the workflow cache instance

- Browse to **Shared Resource > Services > Workflow > Workflow Engine** and verify that the Workflow Engine process is running. If the process is in a stopped state, start the process by clicking the **Run** button. Also ensure that the start type for the service process is set to automatic.



Verify that the Workflow Engine process is running

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

The screenshot shows the System Console interface. On the left, the 'Tree: System' pane is expanded to 'Partitions' > 'egain' > 'Services' > 'Workflow' > 'Workflow Engine'. The main area displays a 'List: Workflow Engine' table with one entry: 'workflow-instance' with description 'Workflow engine instance' and state 'Running'. Below the list is the 'Properties: workflow-instance' section, showing a 'General' tab with the following details:

| Name | Value |
|-----------------|--------------------------|
| Instance name * | workflow-instance |
| Description | Workflow engine instance |
| Start type * | Automatic |

Start the Workflow Engine instance

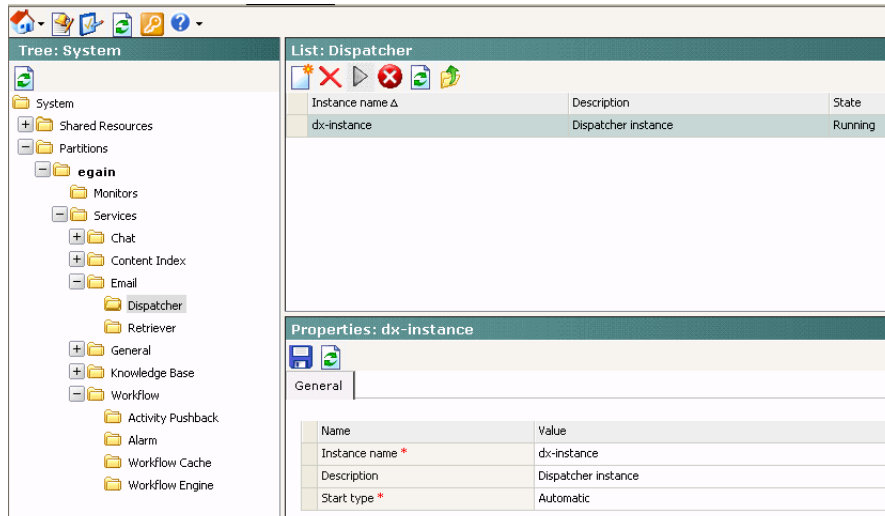
- Browse to **Shared Resource** > **Services** > **Email** > **Dispatcher** and verify that the Dispatcher process is running. If the process is in a stopped state, start the process by clicking the **Run** button. Also ensure that the start type for the service process is set to automatic.

The screenshot shows the System Console interface. On the left, the 'Tree: System' pane is expanded to 'Shared Resources' > 'Services' > 'Email' > 'Dispatcher'. The main area displays a 'List: Dispatcher' table with one entry: 'dx-process' with description 'Dispatcher service process' and state 'Running'. Below the list is the 'Properties: dx-process' section, showing a 'General' tab with the following details:

| Name | Value |
|-------------------------------|----------------------------|
| Name * | dx-process |
| Description | Dispatcher service process |
| Start type | Automatic |
| Maximum number of instances * | 1 |

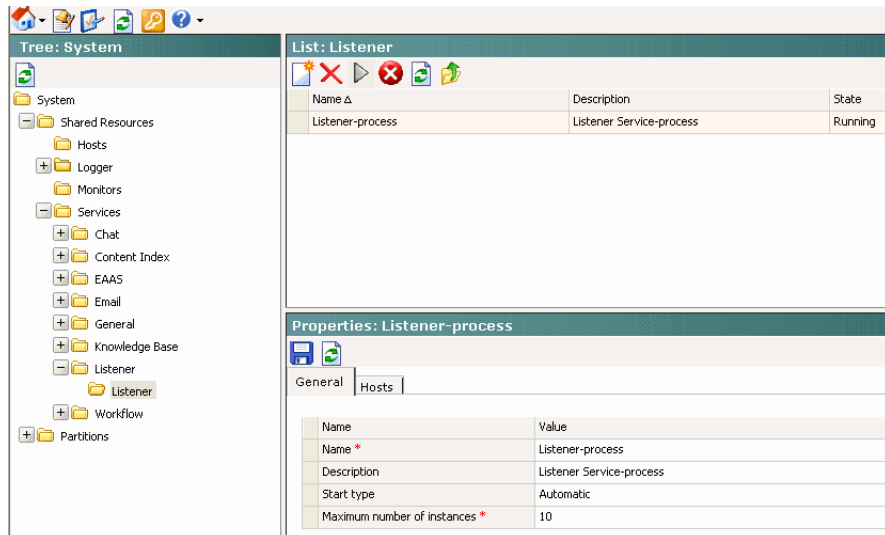
Verify that the Dispatcher process is running

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



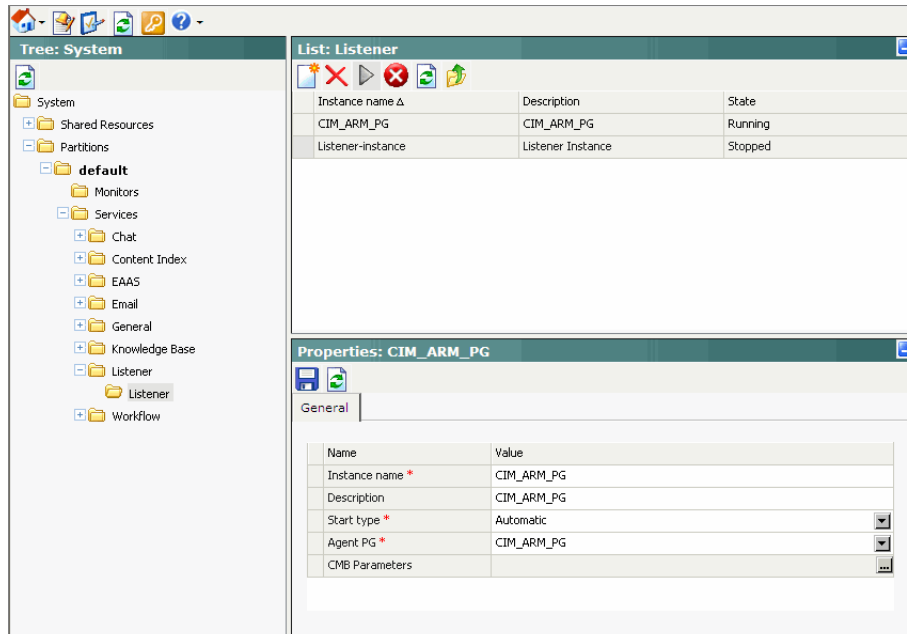
Start the Dispatcher instance

- Browse to **Shared Resource** > **Services** > **Listener** > **Listener** and verify that the Listener process is running. If the process is in a stopped state, start the process by clicking the **Run** button. Also ensure that the start type for the service process is set to automatic.



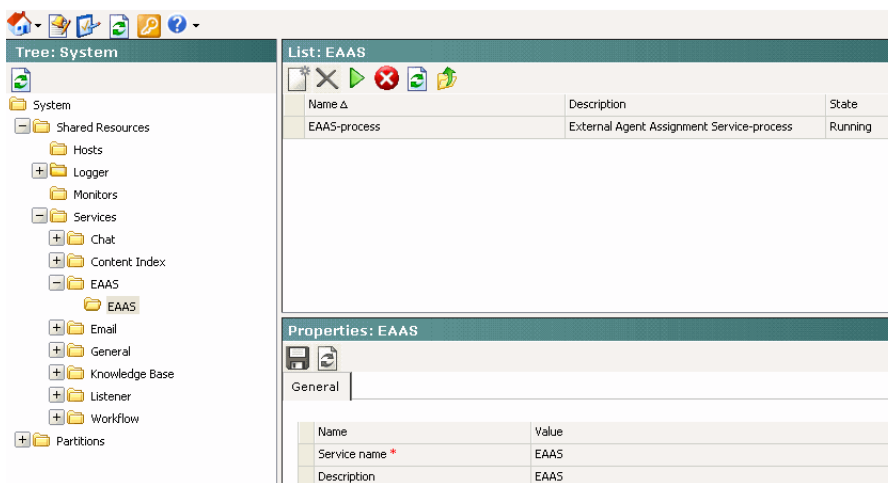
Verify that the Listener process is running

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



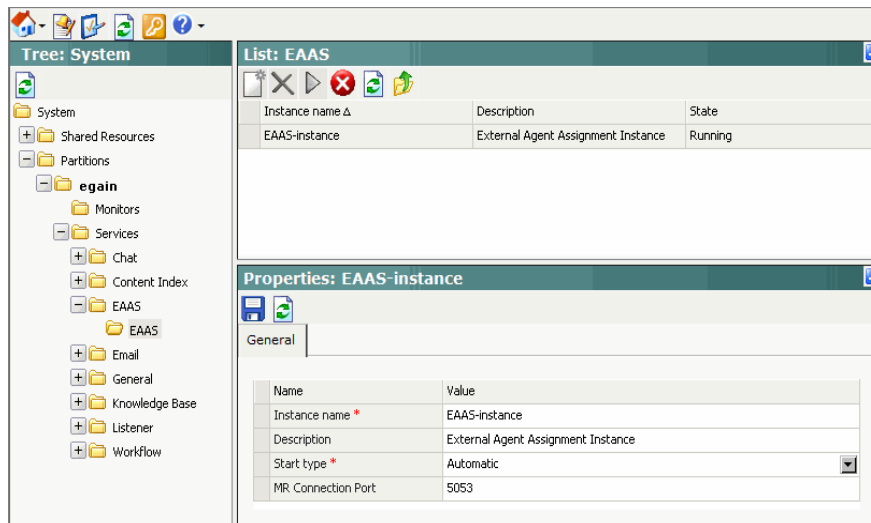
Configure Listener instance

14. Browse to **Shared Resource > Services > EAAS > EAAS** and verify that the EAAS process is running. If the process is in a stopped state, start the process by clicking the **Run** button. Also ensure that the start type for the service process is set to automatic.



Verify that the EAAS process is running

15. Browse to **Partitions > Partition > Services > EAAS > EAAS**. Configure the EAAS instance by providing the MR Connection port number. As a best practice we recommend that you use a port number greater than 2000. Start the EAAS instance. Also ensure that the start type for the instance is set to automatic. Start the EAAS instance.



Start the EAAS instance

Setting up Unified WIM Services

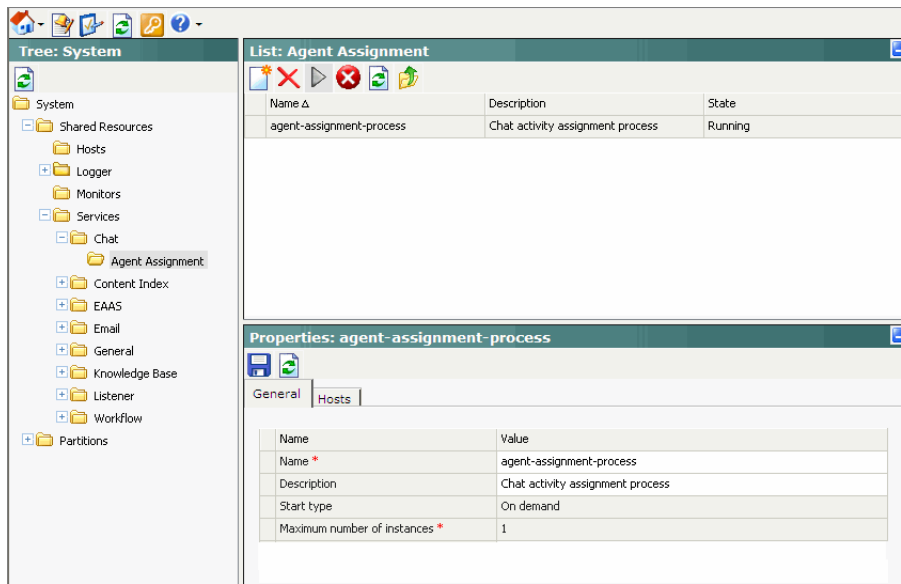
The following services are required for Unified WIM:

- ▶ **Agent Assignment:** Used to initiate chat and collaboration sessions.
- ▶ **External Agent Assignment Service (EAAS):** Identifies new activities that arrive into an external assignment queue, and routes requests for each of these activities to Unified CCE for routing to take place through Unified CCE.
- ▶ **Listener:** Assigns activities to target agents or user groups (skill groups) identified by Unified CCE, and reports the status of both the activity and the agent to Unified CCE throughout the life cycle of the given activity.

To set up these services:

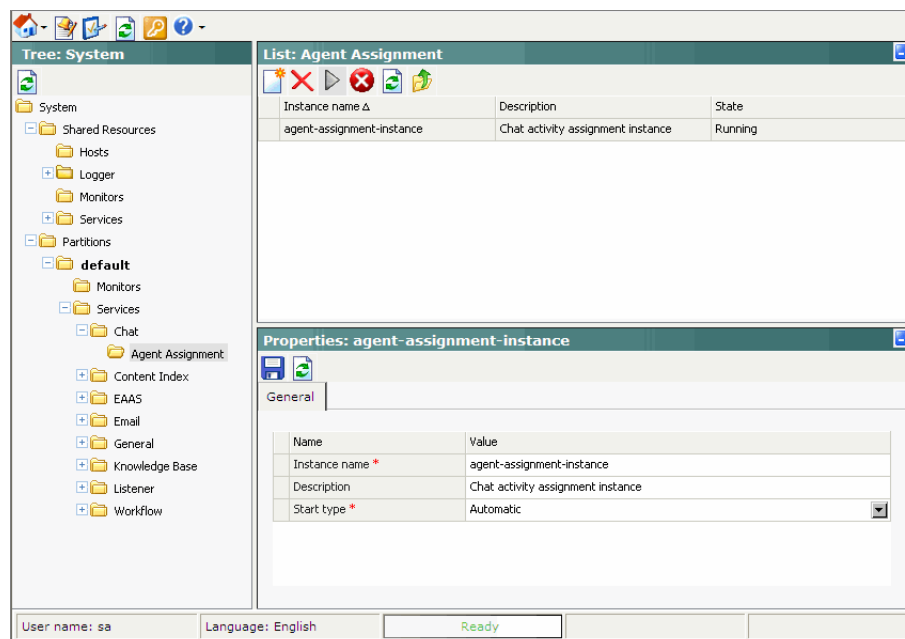
1. Log in to the system as the system administrator from the following URL: http://Unified WIM_Server/system.
2. Select the System Console.

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



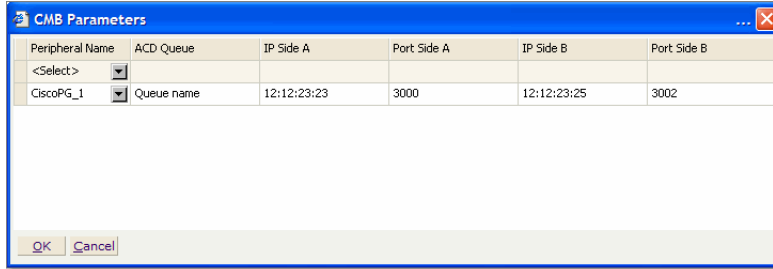
Start the Agent Assignment process

- Browse to **Partitions > Partition > Services > Chat > Agent Assignment** and configure the instance to start automatically. Then start the Agent Assignment instance.



Start the Agent Assignment instance

- Follow the instructions in steps 12-15 in [“Setting up Unified EIM Services”](#) on page 17. In addition to the fields mentioned in [Step 13](#), configure the CMB parameters fields for the listener service instance.



Configure CMB parameters for Listener instance

Setting up Standalone Email Services

The following services are required for standalone email:

- ▶ **Retriever:** Gets incoming emails from configured aliases and parses them.
- ▶ **Workflow Engine:** Applies workflows on emails to automate their routing and handling.
- ▶ **Dispatcher:** Sends outgoing emails out of the system.

To set up these services, follow the instructions in steps 1-11 in [“Setting up Unified EIM Services”](#) on page 17.

Setting up Standalone Chat Services

Use this section only if you are using standalone chat that is not integrated with Unified CCE or a legacy ICM. This section helps you set up processes and instances for the following service:

- ▶ **Agent Assignment:** Used to initiate chat sessions and routes chats to agents.

To set up these services, follow the instructions in steps 1-4 in [“Setting up Unified WIM Services”](#) on page 25.

3 Business Partition

- ▶ [About the Business Partition](#)
- ▶ [Managing the Business Partition](#)

About the Business Partition

The business partition in a system contains all the information for the everyday functioning of the business unit. The installation program creates the default business partition. It generates two URLs: one for accessing the Unified System view and the other to access the business partition. Unified System view and the partition view have separate users. Typically, only system administrators use the Unified System view. All partition administrators and other users of the system work in the business partition.

Managing the Business Partition

You may need to edit the business partition if you want to adapt it to a changing business unit. You can modify the properties of the partition to meet changing requirements.

Managing Service Instances

Increasing the Number of Service Instances

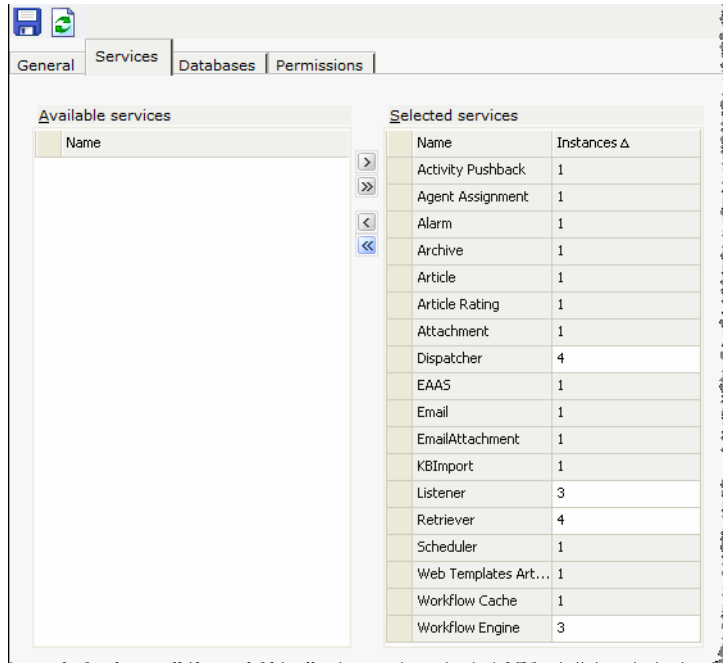
Depending on the nature of your installation and the work load it receives, you may want to increasing the number of certain service instances to improve performance. You can have more than one service instance for the following services:

- ▶ Email services: Retriever and Dispatcher
- ▶ Workflow service: Workflow Engine
- ▶ Listener service

For all other services, only one instance is supported.

To increase the number of instances of a service:

1. In the Tree pane, browse to **System > Partitions**.
2. In the List pane, select a partition.
3. In the Properties pane, go to the Services tab and in the selected instances list increase the number of instances for the services.



Increase number of service instances for the business partition

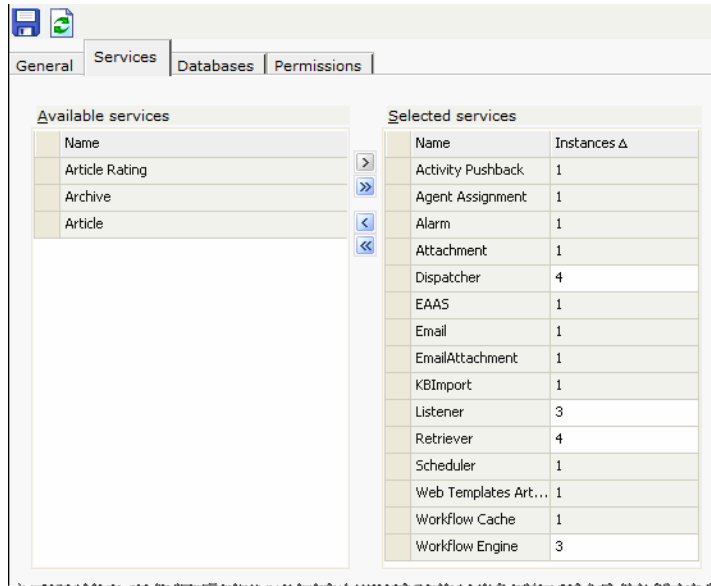
4. Click the **Save**  button.

Removing Service Instances

If the business partition does not need a particular service, remove its service instance from the partition. Once an instance is removed, no user in the partition can start the service instance. Before removing an instance, make sure that the service process is not running.

To remove a service instance:

1. In the Tree pane, browse to **System > Partitions**.
2. In the List pane, select a partition.
3. In the Properties pane, go to the Services tab and from the selected service instances remove the appropriate instance.



Remove service instances not needed for the partition

4. Click the **Save**  button.

Viewing Database Details

You can view database details from the Partitions node in the Tree pane. Except for the details of IPCC primary and secondary databases, you cannot edit information related to any other database from the System Console.

To view the database details:

1. In the Tree pane, browse to **System > Partitions**.
2. In the List pane, select the business partition.
3. In the Properties pane, go to the Databases tab. It shows the details about the following databases:
 - **Customer DB**
 - **Master DB**
 - **Mail DB**
 - **Archive DB**
 - **Archive app DB**
 - **Knowledge DB**
 - **IPCC primary database**
 - **IPCC secondary database**
4. For each of these databases, information on the following attributes is available:
 - **Name:** Name of the database.
 - **Active:** Whether the database is active or not.
 - **Type**

- **Capacity increment**
- **Initial capacity**
- **Maximum capacity**
- **Drive name**
- **User**
- **Password**
- **URL**
- **Targets**
- **Vendors**
- **Drive vendor**

| Name | Value |
|----------------|---------------------|
| customer_db | |
| master_db | Platform_MSSQL_Pool |
| mail_db | y |
| archive_db | basic |
| archive_app_db | CapacityIncrement |
| knowledge_db | InitialCapacity |
| ipcc_db_prim | MaxCapacity |
| ipcc_db_sec | DriverName |
| | User |
| | Password |
| | Url |
| | Targets |
| | Vendor |
| | DriverVendor |

View database details of a partition

Configuring Database Details

Only the database details of the IPCC primary and secondary databases can be edit from the System Console.

To configure the database details:

1. In the Tree pane, browse to **System > Partitions**.
2. In the List pane, select the business partition.
3. In the Properties pane, on to the Databases tab, go to the ipcc_db_prm or ipcc_db_sec section and configure the following properties:
 - **Active:** Set the value as **y**.
 - **User:** Provide the user name to connect to the ICM Admin Workstation DB.
 - **Password:** Provide the password.
 - **URL:** Provide the URL in the format
`jdbc:sqlserver://Host_Name:Port_Number;DatabaseName=Database_Name`

Where

Host_Name: Is the host name of the machine where the ICM Admin Workstation DB is installed.

Port_Number: The port number on which the SQL server looks for the connection request. The default value is 1433.

Database_Name: Name of the ICM Admin Workstation DB.

Assigning Permissions

For the business partition, you can give the following permissions to the system level users.

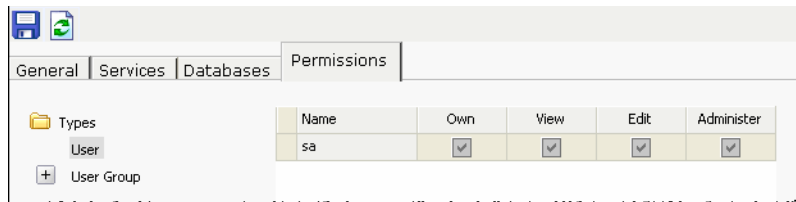
- Own
- View
- Edit
- Administer



Important: Permissions can be given only to users and user groups who have appropriate actions assigned to them. When permissions are given to a user group, all users in that user group get those permissions automatically.

To assign permissions:

1. In the Tree pane, browse to **System > Partitions**.
2. In the List pane, select a partition.
3. In the Properties pane, go to the Permissions tab and assign permissions to the users and user groups on the partition.



Assign permissions to users and user groups

4. Click the **Save**  button.



Managing Hosts

- ▶ [About Hosts](#)
- ▶ [Editing Hosts](#)
- ▶ [Deleting Hosts](#)
- ▶ [Stopping Hosts](#)
- ▶ [Starting Hosts](#)

About Hosts

Hosts can be configured from the System Console for the overall system. These are the physical machines on which software processes will be running. You can access details about the hosts from the **Shared** resources node in the System Console.

Hosts are created during the installation process. As of now a deployment can have only one host.

Editing Hosts

Though you cannot create hosts from the System Console, you can modify the properties of hosts. There are only a very few properties that you can edit from the console.

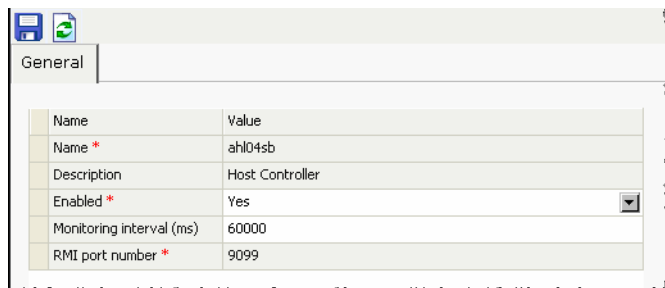
You may want to edit a host property to change its availability in the system. You may also want to monitor the host functions frequently and hence want to change its monitoring interval.

To edit a host:

1. In the Tree pane, browse to **System > Shared Resources > Hosts**.
2. In the List pane, select the host.

The Properties pane refreshes to show the properties of the host.

3. In the Properties pane, go to the General tab. All the properties of the host can't be modified. You can only enable or disable the host, or change its monitoring interval. You can't modify the name, description, and RMI port number of the host.
 - **Name:** Displays the name of the host.
 - **Description:** Displays the description of the host.
 - **Enabled:** By default the host is enabled. Select **No** to disable to host.
 - **Monitoring interval:** Set the monitoring interval in milliseconds. The default value is 60000 milliseconds.
 - **RMI port number:** The RMI post number of the host.



Edit properties of a host

4. Click the **Save**  button.


Deleting Hosts

Although the system allows you to delete hosts, it is advisable not to do so.

Stopping Hosts

Once you stop the host all the service processes running on the host also stop running.


To stop a host:

1. In the Tree pane, browse to **System > Shared Resources > Hosts**.
2. In the List pane, select the host.
3. In the List pane toolbar, click the **Stop**  button.

Starting Hosts

Once you start the host all the service processes for the host do not start running automatically. You have to run the service processes and service instances manually.

To start a host:

1. In the Tree pane, browse to **System > Shared Resources > Hosts**.
2. In the List pane, select the host.
3. In the List pane toolbar, click the **Start**  button.



Services

- ▶ [About Services, Service Processes, and Service Instances](#)
- ▶ [Managing Service Processes](#)
- ▶ [Managing Service Instances](#)

About Services, Service Processes, and Service Instances

Services

Services accomplish specialized functions within the system. For example, a dispatcher service is responsible for sending out emails. Similarly other services perform varied functions for the system. Multiple processes and instances can be created for some of the services.

Services are of following types:

- ▶ Chat service
 - Agent Assignment service
- ▶ Content Index services
 - Attachment service
- ▶ EAAS service
 - EAAS
- ▶ Email services
 - Dispatcher service
 - Retriever service
- ▶ General service
 - Archive service
 - Report service
 - Scheduler service
- ▶ Knowledge Base (KB) services
 - Article Rating service
 - KB Import service
- ▶ Listener service
 - Listener
- ▶ Workflow services
 - Activity Pushback service
 - Alarm service
 - Workflow Cache service
 - Workflow Engine service

Chat Service

- ▶ **Agent Assignment service:** This service is used to initiate chat and collaboration sessions. It also routes chat activities to standalone queues and assigns them to available standalone agents. This service is used for initiating integrated chats and collaboration sessions, however the routing of these activities is done by the EAAS.

Content Index Services

- ▶ **Attachment service:** This service facilitates searches on different text-based attachments. It filters such attachments and stores the text content in a full text-enabled database column. It then indexes the text content periodically. Any search on an attachment is carried out on this index enabling the system to quickly return search results and improve user experience.

External Agent Assignment Services

- ▶ **EAAS:** The external agent assignment service (EAAS) routes email, chat, callback, delayed callback, and blended collaboration activities requests to Unified CCE. EAAS sends a request to Unified CCE for every activity that arrives into an external assignment queue, for the identification of an agent who is available to handle the given activity.

This service can have only one process and instance and neither can be deleted.

Email Services

- ▶ **Dispatcher service:** This service turns the messages that agents write, into emails and sends them out of your Mail system. The dispatcher service acts as a client that communicates with SMTP or ESMTP servers.
- ▶ **Retriever service:** This service is a POP3 or IMAP client that fetches incoming emails from servers. It then turns them into messages that agents can view in their mailbox.

General Services

- ▶ **Archive service:** This service archives the cases and activities from the partition database to the archive database. It also purges data from the archive database.
- ▶ **Reports service:** This service generates the reports, which are scheduled to run automatically or are run manually, and sends notifications to users, if they are configured. Notifications are sent for both scheduled and manually run reports. For running the scheduled reports, the Scheduler service should also be running. The reports service also needs to be running for using the print feature available in the various console. This service can have only one process and instance.
- ▶ **Scheduler service:** This service schedules the messaging and reminder system.

Knowledge Base (KB) Services

- ▶ **Article Rating service:** This service assigns an average rating to each of the articles present in the Knowledge Base. An article's average rating is computed based on its rating given explicitly by the users and the number of times the article was used. The average rating is used for selecting specific articles to be displayed in **Most Popular Articles** folder in KB Console.
- ▶ **KB Import service:** This service imports folders and articles from external file system to the knowledge base. The service imports folders and articles only from the external content folders specified in the knowledge base. The files are imported as knowledge base articles (either as internal or external attachments) and directories as folders. If any file is updated on the external file system, since the last run of service, the service also updates those files in knowledge base.

Listener Services

- ▶ **Listener service:** This service initiates and maintains a reliable channel of communication with the Agent Peripheral Gateway (PG)/ARM interface of Unified CCE. Each instance of this service is dedicated to communicating with an Agent PG, and reports the current state of integrated agents and tasks to the appropriate Agent PG (i.e. the Agent PG to which the relevant agent belongs). For blended collaboration activities, the service opens a channel through which the Listener Instance communicates with CMB. All agent related messages that need to be passed to CMB are forwarded through this channel. These include, but are not limited to agent login events and agent activity assignment events. These events are then used by Unified CCE for reporting purposes.

Workflow Services

- ▶ **Activity Pushback service:** This service is a continuous service that pushes agents' unpinned activities, back into the queue after they have logged out. Those activities get reassigned to other users in the queue.
- ▶ **Alarm service:** This service runs at specific time intervals. While processing a workflow, it determines if any alarm conditions are met. It then performs the relevant actions including sending out any configured notifications or alarms to the user.
- ▶ **Workflow Cache service:** This service maintains and updates the Rules Cache, KB Cache, and Queue Cache in the system. It generates a serialized file that is accessed by all rules engine instances before executing rules.
- ▶ **Workflow Engine service:** This service is the main Rules engine. It uses the cache from serialized files produced by Rules Cache service, and applies rules on activities on the basis of workflows. This service handles the general, inbound, and outbound workflows.

Service Processes

At least one service process for each service should be running to enable the basic functioning of the system. Service processes can be set to start automatically, or can be started manually by the system administrator.

Service Instances

Service instances are derivatives of service processes. Configure service instances within the business partition to accomplish specific functions. For example, in an installation that is used to manage five different email aliases you could configure two service instances of the retriever service process and assign three aliases to one instance and two aliases to the other.


Managing Service Processes

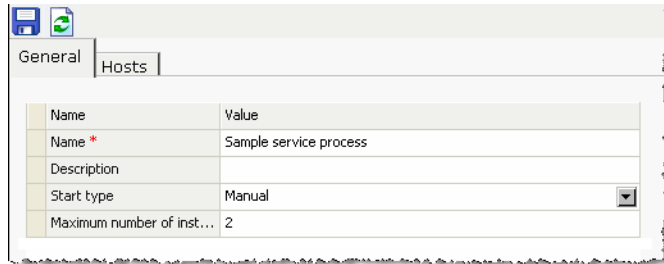
For each service, a service process is provided in the system. In addition to these you can create new service processes. You have to start a service process before the system can use that process.

Creating Service Processes


Before creating a service process, estimate your system requirements well. Depending on your needs, you can create the number and type of service processes you require.

To create a service process:

1. In the Tree pane, browse to **System > Shared Resources > Services**.
2. Browse to the service for which you want to create a new process.
3. In the List pane toolbar, click the **New**  button.
4. In the Properties pane, go to the General tab and provide the following details.
 - **Name:** Type a name for the process. This is required information.
 - **Description:** Provide a brief description.
 - **Start type:** From the dropdown list, select a start type for the service process. The following three options are available.
 - **Manual:** The service process has to be started manually by the system administrator.
 - **Automatic:** The service process is started automatically by the system when the application is started.
 - **On demand:** The service process is started by the system when the service instance associated with the process is started.
 - **Maximum number of instances:** Type the maximum number of instances this service process can have. This option is available only for those services that can have more than one instance.




Set the general properties

- Next, go to the Hosts tab and select the host from the available hosts list. Ignore the other options as they are not available in this release.
- Click the **Save**  button.

Deleting Service Processes

The system will allow you to delete certain service processes that are not required in the system. Before you delete the service process make sure it is not running. Not all service processes in the system can be deleted.

To delete a service process:

- In the Tree pane, browse to **System > Shared Resources > Services**.
- Browse to the service for which you want to delete a process. In the List pane select the service process. Stop the service process if it is running.
- In the List pane toolbar, click the **Delete**  button.


Increasing the Number of Instances for Service Processes

The system allows you to create more than one instance of certain service processes to help increase performance. As a system administrator you can create these instances from the System Console. The following services can have more than one instance:

- ▶ Email services: Retriever and Dispatcher
- ▶ Workflow service: Workflow Engine
- ▶ Listener service

You can also set the maximum number of service instances that can be created for each of the above services processes.

To increase the number of instances for a service process:


- In the Tree pane, browse to **System > Shared Resources > Services**.
- Browse to the service for which you want to increase the number of service instances.
- In the Properties pane, on the General tab go to the **Maximum number of instances** field, and type the maximum number of instances this service process can have.
- Click the **Save**  button.

5. Stop and start the service process.

Starting Service Processes

Unless a service process is configured to start automatically when a system is running, you have to manually start the particular process when you require it. Every time you start the service process, you need to manually start the instances for that service.

To start a service process:


1. In the Tree pane, browse to **System > Shared Resources > Services**.
2. Browse to the service for which you want to start a process. In the List pane select the service process.
3. In the List pane toolbar, click the **Start**  button.

The process starts on the selected hosts.

Stopping Service Processes

Stop the service process if it is not needed. This frees up system resources. Sometimes you may be required to stop and start a service process after making changes to its properties. For example, when you increase or decrease the number of service instances that can be associated with a particular service process, you must stop and start that service process.

To stop a service process:

1. In the Tree pane, browse to **System > Shared Resources > Services**.
2. Browse to the service for which you want to stop a process. In the List pane select the service process.
3. In the List pane toolbar, click the **Stop**  button.

The process stops working on the selected hosts.



Important: Once the service process is stopped, all service instances also stop.

Managing Service Instances


Service instances are specific to the business partition. You can manage all the activities related to instances from the business partition. You can also create and delete instances as required.

Creating Service Instances

By default, one service instance is provided for each service in the system. The system allows you to create additional service instances for certain services. The services that can have more than one instance running at a time are:

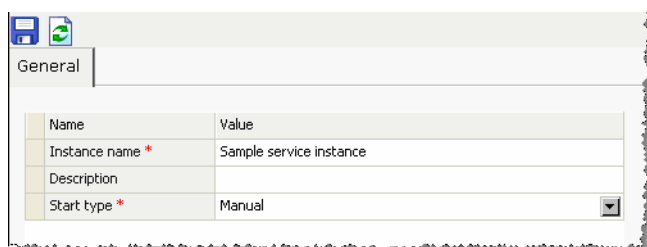
- ▶ Email services: Retriever and Dispatcher
- ▶ Workflow service: Workflow Engine
- ▶ Listener Service

To create a service instance:

1. In the Tree pane, browse to **System > Partition > *Partition_Name* > Services**.
2. Browse to the service for which you want to create a new instance.
3. In the List pane toolbar, click the **New**  button.

The Properties pane refreshes to show the attributes of the new process.

4. In the Properties pane, go to the General tab and provide the following details.
 - **Instance name:** Type a name for the instance. This is required information.
 - **Description:** Provide a brief description.
 - **Start type:** From the dropdown list, select a start type for the instance. The following two options are available.
 - **Manual:** The service instance has to be started manually by the system administrator.
 - **Automatic:** The service instance is started automatically by the system when the application is started.




The screenshot shows a 'General' tab in a properties window. It contains a table with the following data:

| Name | Value |
|-----------------|-------------------------|
| Instance name * | Sample service instance |
| Description | |
| Start type * | Manual |

Set the general properties

5. For retriever service instances, there is an additional Input tab. On the Input tab, select the aliases from the available list of aliases.
6. For the EAAS Service, there is an additional MR Connection port field. Refer to the following section for more details: [“Configuring the MR Connection Port for an EAAS Service Instance”](#) on page 46.

7. For the listener service, two additional fields have to be configured. These are the Agent PG and CMB Parameters fields. For more information about these fields refer to the [“Configuring a Listener Service Instance” on page 47](#)
8. Click the **Save**  button.




Important: The number of instances for a given service should tally with the maximum number of instances defined for the service process in Shared Resources. For details refer to the following section: [“Increasing the Number of Instances for Service Processes” on page 42.](#)

Deleting Service Instances

You can delete a service instance if it is not required anymore or occupies system resources.

To delete a service instance:

1. In the Tree pane, browse to **System > Partition > *Partition_Name* > Services**.
2. Browse to the service for which you want to delete an instance. In the List pane select the service instance. Stop the service instance if it is running.
3. In the List pane toolbar, click the **Delete**  button.


Starting Service Instances

Unless a service instance is configured to start automatically when a system is running, you have to manually start the particular instance when you require it. Every time you start the service process, you need to manually start the instances for that service in the business partition.

When you create additional instances for a service, you can start those instances only after you do the following.

- ▶ Increase the number of instances that can be associated with the service process. And, restart the service process. For details, see [“Increasing the Number of Instances for Service Processes” on page 42.](#)
- ▶ Increase the number of instances that can be running in the business partition. For details, see [“Increasing the Number of Service Instances” on page 29.](#)

To start a service instance:

1. In the Tree pane, browse to **System > Partition > *Partition_Name* > Services**.
2. Browse to the service for which you want to start an instance. In the List pane select the service instance.
3. In the List pane toolbar, click the **Start**  button.

The instance starts running.




Important: More than one service instance cannot be started on a business partition, except for Retriever, Dispatcher, Listener, and Rules.

Stopping Service Instances

Stop the service instance if it is not needed. This frees up the system resources. Some times you need to stop and start a service instance after making some changes in its properties. For example, when you add an alias to a retriever instance, you need to stop and start the retriever instance and all the dispatcher instances for the business partition.

To stop a service instance:


1. In the Tree pane, browse to **System > Partition > *Partition_Name* > Services**.
2. Browse to the service for which you want to stop an instance. In the List pane select the service instance.
3. In the List pane toolbar, click the **Stop**  button.

The instance stops running.

Adding Aliases to Retriever Instances

You can start the retriever instance only after you add an alias to the retriever instance. A retriever instance can have any number of aliases, but one alias can be associated with only one instance.

To add aliases to a retriever instance:

1. In the Tree pane, browse to **System > Partition > *Partition_Name* > Services > Email > Retriever**.
2. In the List pane, select the retriever instance.
3. In the Properties pane, go to the Input tab and select the aliases to be associated with this instance.
4. Click the **Save**  button.
5. Stop and start the retriever instance. The retriever picks emails from the alias only after you restart the retriever instance.

Configuring the MR Connection Port for an EAAS Service Instance

This is the port used by Unified EIM and WIM when initializing a server socket connection with Unified CCE to listen to incoming connections from the Media Routing Peripheral Gateway (MR PG) of Unified CCE and is a pre-requisite for sending new activity requests for routing through Unified CCE.

The port number entered here should match the corresponding value that is entered at the time of setting up the Media Routing Peripheral Interface Manager (MR PIM) in Unified CCE. As a best practice we recommend that you use a port number greater than 2000.

Enter this value manually *after* starting Unified EIM and WIM, and *before* starting the EAAS process and instance from the System Console.

If this value is modified later (based on a modification within the MR PIM) you must restart both the service process and the instance.

Configuring a Listener Service Instance

In addition to the standard fields mentioned in the [“Creating Service Instances”](#) on page 44, the following fields are displayed for each listener service instance:

- ▶ **Agent PG:** This is a required field. From the dropdown list, select the Agent PG to which the listener instance should connect. For auto-configured listener instances, this field will be configured automatically and will show the name of the Agent PG that was selected in the integration wizard.
- ▶ **CMB Parameters:** This field needs to be configured only for blended collaboration type of activities. Provide the following details in the CMB Parameters window.
 - **Peripheral Name:** Name of the peripheral associated with the Agent PG configured for the listener service instance.
 - **ACD Queue:** The name of the queue configured on ACD. Set this value only if you are using an ACD.
 - **IP Side A:** IP address of the Side A CMB. The Listener service uses this IP address to connect to the Side A CMB.
 - **Port Side A:** Port on which Side A CMB is listening. The Listener service uses this port to connect to the Side A CMB.
 - **IP Side B:** IP address of the Side B CMB. This is optional. Need to be configured only to handle failover. The Listener service uses this IP address to connect to the Side B CMB.
 - **Port Side B:** Port on which Side B CMB is listening. The Listener service uses this port to connect to the Side B CMB.

After you have configured the required values, and saved your changes, you must restart the service process and instances.



Loggers and Appenders

- ▶ [About Loggers and Appenders](#)
- ▶ [Managing Loggers](#)
- ▶ [Managing Appenders](#)

About Loggers and Appenders

Logging is a mechanism for capturing log messages as they are encountered while the product is running. Messages are logged at seven trace levels and they are:

- ▶ **1 - Fatal:** This level identifies critical messages. If messages are getting logged at this level it generally indicates that some major component or functionality of the product is not working.
- ▶ **2 - Error:** This level identifies problems that cause certain actions in the product to fail.
- ▶ **3 - Warn:** This level identifies potential problem conditions in the product that might need attention.
- ▶ **4 - Info:** This level logs information messages that are required to check the sanity of the system.
- ▶ **5 - Perf:** This level is used by performance monitors that run in the product. Any performance related information is captured at this level.
- ▶ **6 - Dbquery:** This level logs database queries that are executed in the product.
- ▶ **7 - Debug:** This level logs messages to identify the complete flow of the code. This is the highest level of logging and produces maximum number of log messages.

These trace levels are associated with loggers and appenders. The details are described in the following sections.

Loggers

A logger is an object that captures log messages as they occur, generates log statements in a specified format, and saves them in the process memory. The level of logs to be captured by a logger is determined by the trace level of the logger. For example, if the trace level of a logger is set to 5 - Perf, the messages logged at the following levels are captured by the logger: 1 - Fatal, 2 - Error, 3 - Warn, 4 - Info, and 5 - Perf.

The system comes with six loggers. You cannot delete these loggers or add new loggers. However, you can adjust the trace levels of loggers to decide what all type of messages the logger should capture.

List of Loggers Available in the System

1. **com.egain:** The default trace level is set to 2-Error.
2. **com.cisco:** The default trace level is set to 2-Error.
3. **com.egain.knowledge.central.importtask:** This logger is not in use.
4. **com.egain.knowledge.export:** This logger is not in use.
5. **egain.dal.connpool:** The default trace level is set to 7-Debug.
6. **egain.dal.querytimeout:** The default trace level is set to 7-Debug.

Appenders

An appender is an object that saves the messages generated by the logger in the log file associated with the appender. The level of logs to be saved in a log file is determined by the trace level of the appender. For example, if the trace level of an appender is set to 5 - Perf, the messages logged at the following levels are saved by the appender: 1 - Fatal, 2 - Error, 3 - Warn, 4 - Info, and 5 - Perf.

Appenders are associated with loggers, and more than one appender can be attached to a logger. It is important to note that since appenders are attached to loggers, the trace level of appenders cannot be set higher than the trace level of the logger with which it is associated. This is because, if the logger is capturing messages only till a certain level, then the messages above that level will not be available to the associated appender to write in a log file.

An appender and an associated log file is created for each java process in the product. The first time the product is started, appenders and log files are created only for the processes which start at that time. As more processes are started, appenders and log files for those process are created. And, if a process is not started, the appender and log file for that process is never created.

The names of the appenders are created in the following format: *ServerName_ProcessName*, where *ServerName* is the name of the server where the java process is running and *ProcessName* is the name of the java process.

Similarly, the names of the log files are created in the following format: *eg_log_ServerName_ProcessName.log*, where *ServerName* is the name of the server where the java process is running and *ProcessName* is the name of the java process.

If you rename a process and restart it, a new appender and log file with the new process name is created for the process. Also note that the old appender for that process will always show in the list of appenders.

When a log file reaches its maximum size (that is 5 MB), the file is backed-up as “*File_Name.log.<number starting from 1>*” (for example, *eg_log_V22W2_Application Server.log.1*, *eg_log_V22W2_Application Server.log.2*, etc) and a new log file is created.

List of Appenders Available in the System

This section provides a list of the default appenders available in the system. For each appender, we list the loggers used by it and the name of the log file in which it records information.

| # | Component | Appender name | Log file name | Logger name |
|----|------------------------------------|--|---|------------------------|
| 1. | Installation program | <i>Server_Name_eGainInstaller</i> | <i>eg_log_Server_Name_eGainInstaller.log</i> | com.egain |
| 2. | System monitoring and health check | <i>dal_connpool</i> | <i>eg_log_dal_connpool.log</i> | egain.dal.connpool |
| 3. | System monitoring and health check | <i>dal_query_timeout</i> | <i>eg_log_dal_query_timeout.log</i> | egain.dal.querytimeout |
| 4. | Distributed Services Manager (DSM) | <i>Services_Server_Name_DSMController</i> | <i>eg_log_Services_Server_Name_DSMController.log</i> | com.egain |
| 5. | Distributed Services Manager (DSM) | <i>Services_Server_Name_dsm-registry</i> | <i>eg_log_Services_Server_Name_dsm-registry.log</i> | com.egain |
| 6. | Distributed Services Manager (DSM) | <i>Services_Server_Name_HostController</i> | <i>eg_log_Services_Server_Name_HostController.log</i> | com.egain |
| 7. | Distributed Services Manager (DSM) | <i>Services_Server_Name_license-manager</i> | <i>eg_log_Services_Server_Name_license-manager.log</i> | com.egain |
| 8. | Distributed Services Manager (DSM) | <i>Services_Server_Name_ServerMonitoring</i> | <i>eg_log_Services_Server_Name_ServerMonitoring.log</i> | com.egain |

| # | Component | Appender name | Log file name | Logger name |
|-----|--|---|--|--|
| 9. | Distributed Services Manager (DSM) | <i>Services_Server_Name_ServiceController</i> | <i>eg_log_Services_Server_Name_ServiceController.log</i> | com.egain |
| 10. | Application server | <i>Application_Server_Name_Application Server</i> | <i>eg_log_Application_Server_Name_Application Server.log</i> | com.egain |
| 11. | Agent Assignment service process | <i>Services_Server_Name_agent-assignment-process</i> | <i>eg_log_Services_Server_Name_agent-assignment-process.log</i> | com.egain |
| 12. | Alarm service process | <i>Services_Server_Name_alarm-rules-process</i> | <i>eg_log_Services_Server_Name_alarm-rules-process.log</i> | com.egain |
| 13. | Archive service process | <i>Services_Server_Name_archive_process</i> | <i>eg_log_Services_Server_Name_archive_process.log</i> | com.egain |
| 14. | Activity Pushback service process | <i>Services_Server_Name_auto-pushback-process</i> | <i>eg_log_Services_Server_Name_auto-pushback-process.log</i> | com.egain |
| 15. | Dispatcher service process | <i>Services_Server_Name_dx-process</i> | <i>eg_log_Services_Server_Name_dx-process.log</i> | com.egain |
| 16. | KB Import service process | <i>Services_Server_Name_import-process</i> | <i>eg_log_Services_Server_Name_import-process.log</i> | com.egain |
| 17. | Article Rating service process | <i>Services_Server_Name_kb-article-rating-process</i> | <i>eg_log_Services_Server_Name_kb-article-rating-process.log</i> | com.egain |
| 18. | Attachment service process | <i>Services_Server_Name_kb-attachment-cs</i> | <i>eg_log_Services_Server_Name_kb-attachment-cs.log</i> | com.egain |
| 19. | Report service process | <i>Services_Server_Name_report-process</i> | <i>eg_log_Services_Server_Name_report-process.log</i> | com.egain |
| 20. | Workflow Cache service process | <i>Services_Server_Name_rules-cache-process</i> | <i>eg_log_Services_Server_Name_rules-cache-process.log</i> | com.egain |
| 21. | Workflow Engine service process | <i>Services_Server_Name_rules-process</i> | <i>eg_log_Services_Server_Name_rules-process.log</i> | com.egain |
| 22. | Retriever service process | <i>Services_Server_Name_rx-process</i> | <i>eg_log_Services_Server_Name_rx-process.log</i> | com.egain |
| 23. | Scheduler service process | <i>Services_Server_Name_scheduler-process</i> | <i>eg_log_Services_Server_Name_scheduler-process.log</i> | com.egain |
| 24. | Cisco Interaction Manager Integration Wizard | <i>File_Server_Name_ui_config</i> | <i>eg_log_File_Server_Name_ui_config.log</i> | com.cisco |
| 25. | EAAS service process | <i>Services_Server_Name_EAAS-process</i> | <i>eg_log_Services_Server_Name_EAAS-process.log</i> | com.cisco |
| 26. | Listener service process | <i>Services_Server_Name_Listener-process</i> | <i>eg_log_Services_Server_Name_Listener-process.log</i> | com.cisco |
| 27. | Not in use | knowledge_export | eg_log_knowledge_export.log | com.egain.knowledge.export |
| 28. | Not in use | knowledge_import | eg_log_knowledge_import.log | com.egain.knowledge.central.importtask |
| 29. | Not in use | <i>Services_Server_Name_ss-article-rating-process</i> | <i>eg_log_Services_Server_Name_ss-article-rating-process.log</i> | com.egain |

Managing Loggers

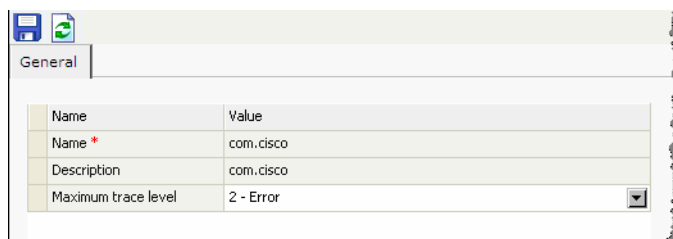
The system allows you to view the properties of loggers and change their trace level. You cannot create new loggers or delete existing ones.

Viewing Loggers

You can view loggers only if the “View loggers” or “Edit loggers” action is assigned to you.

To view the properties of a logger:

1. In the Tree pane, browse to **System > Shared Resources > Logger > Loggers**.
2. In the List pane, select a logger.
3. In the Properties pane, you can view the following details of the logger. Other than the trace level of the logger, you cannot change any other property of the logger.
 - **Name:** The name of the logger.
 - **Description:** The description of the logger.
 - **Maximum trace level:** The maximum level of logging done by the logger. For more details, see [“Changing the Trace Level of Loggers” on page 52](#).



View the general properties

Changing the Trace Level of Loggers

You can edit loggers only if the “Edit loggers” action is assigned to you.



Important: It is advised that you do not change the trace level until and unless Cisco TAC asks you to do so.

To change the trace level of a logger:

1. In the Tree pane, browse to **System > Shared Resources > Logger > Loggers**.
2. In the List pane, select the logger you want to edit.
3. In the Properties pane, change the value in the **Maximum trace level** field. The options available are:
 - **1 - Fatal:** This level identifies critical messages. If messages are getting logged at this level it generally indicates that some major component or functionality of the product is not working.
 - **2 - Error:** This level identifies problems that cause certain actions in the product to fail.

- **3 - Warn:** This level identifies potential problem conditions in the product that might need attention.
- **4 - Info:** This level logs information messages that are required to check the sanity of the system.
- **5 - Perf:** This level is used by performance monitors that run in the product. Any performance related information is captured at this level.
- **6 - Dbquery:** This level logs database queries that are executed in the product.
- **7 - Debug:** This level logs messages to identify the complete flow of the code. This is the highest level of logging and produces maximum number of log messages.

If Maximum trace level is set to 5-perf, the messages with trace levels 1 - Fatal, 2 - Error, 3 - Warn, 4 - Info, and 5 - Perf are logged.

4. Click the **Save**  button.

Managing Appenders

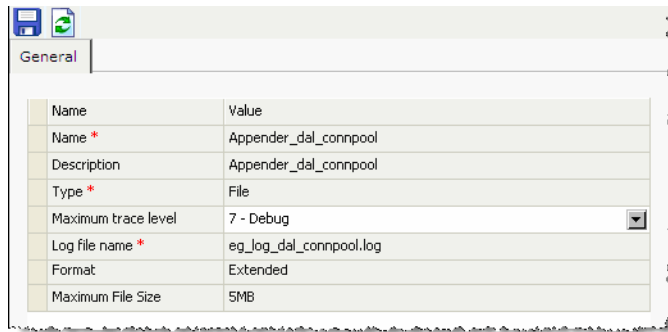
The system allows you to view the properties of appenders and change their trace level. You cannot create new appenders or delete existing ones.

Viewing Appenders

You can view appenders only if the “View appender” or “Edit appender” action is assigned to you.

To view the properties of an appender:

1. In the Tree pane, browse to **System > Shared Resources > Logger > Appenders**.
2. In the List pane, select an appender.
3. In the Properties pane, you can view the following details of the appender. Other than the trace level of the appender, you cannot change any other property of appenders.
 - **Name:** The name of the appender.
 - **Description:** The description of the appender.
 - **Type:** The type of appender. The value is set to **File**, which means that appender stores all messages in a log file.
 - **Maximum trace level:** The maximum level of logging done by the appender. For more details, see [“Changing the Trace Level of Appenders” on page 54](#).
 - **Log file name:** The name of the log file in which the appender records the log messages.
 - **Format:** The format of logging done by the appender. The value in this field is set to **Extended**, which means that complete details of the log message are stored in the log file.
 - **Maximum File Size:** The maximum size of the log file. The value is set to 5 MB.



View the general properties

Changing the Trace Level of Appenders

You can change the trace level of appenders only if the “Edit appender” action is assigned to you. Since appenders are attached to loggers, the trace level of appenders cannot be set higher than the trace level of the logger with which it is associated. This is because, if the logger is capturing messages only till a certain level, then the messages above that level will not be available to the associated appender to write in a log file.



Important: It is advised that you do not change the trace level until and unless Cisco TAC asks you to do so.

To change the trace level of an appender:

1. In the Tree pane, browse to **System > Shared Resources > Logger > Appenders**.
2. In the List pane, select the appender you want to edit.
3. In the Properties pane, change the value in the **Maximum trace level** field. The options available are:
 - **1 - Fatal:** This level identifies critical messages. If messages are getting logged at this level it generally indicates that some major component or functionality of the product is not working.
 - **2 - Error:** This level identifies problems that cause certain actions in the product to fail.
 - **3 - Warn:** This level identifies potential problem conditions in the product that might need attention.
 - **4 - Info:** This level logs information messages that are required to check the sanity of the system.
 - **5 - Perf:** This level is used by performance monitors that run in the product. Any performance related information is captured at this level.
 - **6 - Dbquery:** This level logs database queries that are executed in the product.
 - **7 - Debug:** This level logs messages to identify the complete flow of the code. This is the highest level of logging and produces maximum number of log messages.

If Maximum trace level is set to 5-perf, the messages with trace levels 1 - Fatal, 2 - Error, 3 - Warn, 4 - Info, and 5 - Perf are logged, provided they have been considered for logging by the logger to which this appender is attached.

4. Click the **Save**  button.

7 Monitors

- ▶ [About Monitors](#)
- ▶ [Configuring Monitors](#)
- ▶ [Deleting Monitors](#)
- ▶ [Starting Monitors](#)

About Monitors

Monitors enable you to constantly monitor the important resources in your system. At the shared resources level you can monitor the hosts and service processes, and at the business partition level you can monitor service instances. For each monitor you specify the objects you want to monitor, i.e. the hosts, service processes, or service instances, and the attributes of the objects to be monitor. For each object, different attributes are available for monitoring. For example, you can monitor the free bytes, start time, stop time, and state of hosts.

Host Monitors

Using host monitors, you can monitor the various components of the application, database, web, and services servers. For each of these servers you can monitor the various attributes like the state of the host, and its start and stop time. You can configure a single monitor for all the servers or you can configure a different monitor for each server. Also, while configuring the monitors you can decide if you want to monitor all the attributes or selective attributes.

Objects available for monitoring

- ▶ *Host_name* - DSM Controller
- ▶ *Host_name* - Host Controller
- ▶ *Host_name* - RMI Registry Server
- ▶ *Host_name* - RMID Registry Server
- ▶ *Host_name* - Application Server
- ▶ *Host_name* - Messaging Server
- ▶ *Host_name* - Web Server
- ▶ *Database_server_name* - Database server

Attributes available for monitoring

- ▶ **Host ID:** ID of the host being monitored.
- ▶ **Host Name:** Name of the host being monitored.
- ▶ **Free bytes:** Disc space available on the host.
- ▶ **State:** State of the host. The state can be waiting, running, or stopped.
- ▶ **Status description:** Description of the state of the server.
- ▶ **Start Time:** Time when the host was started.
- ▶ **Stop Time:** Time when the host was stopped.
- ▶ **Last Ping Time:** Last time the DSM pinged the host.

Service Process Monitors

Using service process monitors you can monitor if the service processes are running as desired or not. For each service process you can monitor the various attributes like the state of the process, and its start and stop time. You can configure a single monitor for all the service processes or you can configure a different monitor for each service process. Also, while configuring the monitors you can decide if you want to monitor all the attributes or selective attributes.

Attributes available for monitoring

- ▶ **Host ID:** ID of the host on which the service process is running.
- ▶ **Host Name:** Name of the host on which the service process is running.
- ▶ **Process ID:** ID of the service process being monitored.
- ▶ **Process Name:** Name of the service process being monitored.
- ▶ **State:** State of the process. The state can be waiting, running, or stopped.
- ▶ **Start Time:** Time when the service process was started.
- ▶ **Stop Time:** Time when the service process was stopped.
- ▶ **Last Ping Time:** Last time the DSM pinged the service process.

Service Instance Monitors

Using service instance monitors you can monitor if the service instances for the business partition are running as desired or not. For each service instance you can monitor the various attributes like the state of the instance, and its start and stop time. You can configure a single monitor for all the service instances or you can configure a different monitor for each service instance. Also, while configuring the monitors you can decide if you want to monitor all the attributes or selective attributes.

Attributes available for monitoring

- ▶ **Host ID:** ID of the host on which the service process is running.
- ▶ **Host Name:** Name of the host on which the service process is running.
- ▶ **Instance ID:** ID of the service instance being monitored.
- ▶ **Instance Name:** Name of the service instance being monitored.
- ▶ **Process ID:** ID of the service process with which the instance is associated.
- ▶ **Process Name:** Name of the service process with which the instance is associated.
- ▶ **State:** State of the instance. The state can be waiting, running, or stopped.
- ▶ **Last Run Time:** Time when the instance was last run.
- ▶ **Start Time:** Time when the service instance was started.
- ▶ **Stop Time:** Time when the service instance was stopped.
- ▶ **Processed in last run:** Number of activities processed when the instance last ran.
- ▶ **Processing Time (ms):** Time taken to process the activities.

- ▶ **Pending:** Number of pending email.
- ▶ **Emails Skipped:** Number of skipped emails.
- ▶ **Throughput:** Total number of activities processed since the instance was started.
- ▶ **Unable to Send:** Number of emails unable to send.

Attributes available for monitoring for aliases


- ▶ **Alias name:** Name of the alias.
- ▶ **Instance ID:** ID of the instance with the alias is associated.
- ▶ **State**
- ▶ **Throughput**
- ▶ **Pending**
- ▶ **Last Run**
- ▶ **Emails Skipped**

Configuring Monitors

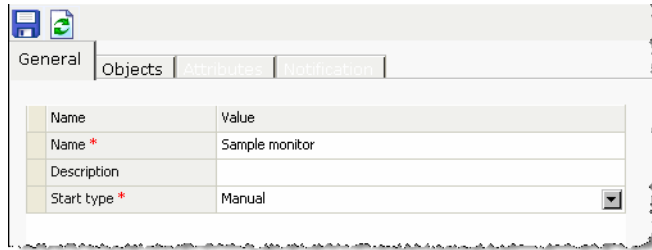
Create different monitors to enable periodic checks on the system resources and business partition resources. These monitors help you keep an account of which system resource is running. Configure monitors such that only the required attributes are displayed in results.

You can configure the monitor to keep running automatically all the time, or you can configure them to run automatically every time you log in to the application. If you do not want to run the monitors automatically, run them manually whenever you need them.


To configure a monitor:

1. In the Tree pane, browse to the **Monitors** node.
 - If it is a shared resource monitor, browse to **System > Shared Resources > Monitors**.
 - If it is a partition monitor, browse to **System > Partition > *Partition_Name* > Monitors**.
2. In the List pane toolbar, click the **New**  button.

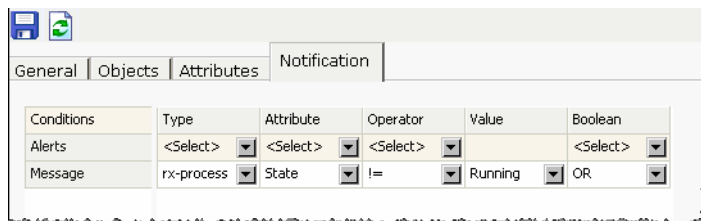
The Properties pane refreshes to show the attributes of the new monitor.
3. In the Properties pane, go to the General tab and provide the following details.
 - **Name:** Type a name for the monitor. This is required information.
 - **Description:** Provide a brief description.
 - **Start type:** From the dropdown list, select a start type for the monitor. The following three options are available.
 - **Manual**
 - **Automatic**
 - **On log in**



Set the general properties

4. Next, go to the Objects tab and select the object to be monitored.
 - For shared resources monitors, select from the list of available hosts and service processes.
 - And, for partition resources, select from the list of available service instances.
5. Next, go to the Attributes tab and select the attributes of the objects to be monitored.
6. Click the **Save**  button.

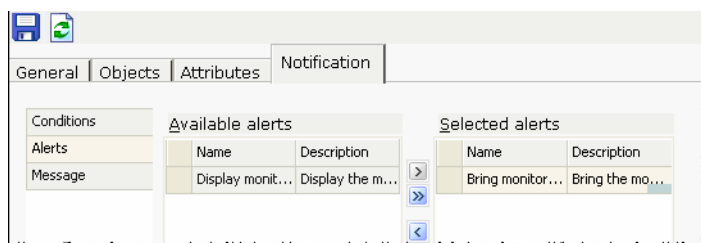
Once you save the monitor the Notification tab is enabled.
7. On the Notification tab, in the Conditions section, specify the condition when a notification should be sent.



Configure conditions for notification

Once you specify the condition, the Alerts and Message sections are enabled.

8. Next, in the Alerts section, you can set the alert type as:
 - **Display monitor window**
 - **Bring monitor window to the front**

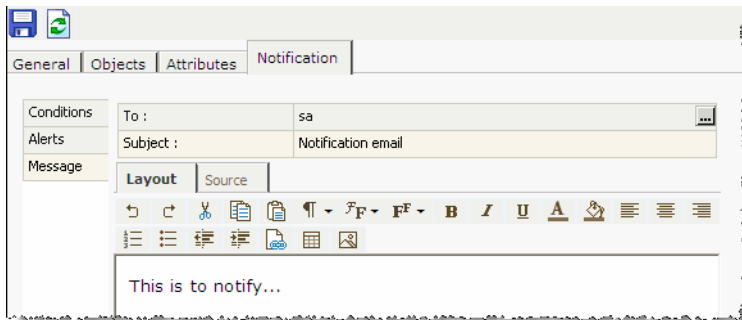


Select alert types

9. Lastly, on the Notification tab, in the Messages section, specify the following.
 - The users to whom you want to send a message. You can send messages to internal user accounts or external email addresses.
 - The subject of the message.

- The content of the message. From the Source tab you can view and edit the HTML code for the content of the message.

This message is sent when the conditions configured in the Conditions section are met.




Create a custom message

10. Click the **Save**  button.

Deleting Monitors

Delete the monitor if you do not want to use it any more.


To delete a monitor:

1. In the Tree pane, browse to the **Monitors** node.
 - If it is a shared resource monitor, browse to **System > Shared Resources > Monitors**.
 - If it is a partition monitor, browse to **System > Partition > *Partition_Name* > Monitors**.
2. In the List pane, select the monitor you want to delete.
3. In the List pane toolbar, click the **Delete**  button.

Starting Monitors

You can configure the monitor to keep running automatically all the time, or you can configure them to run automatically every time you log in to the application. If you do not want to run the monitors automatically, start them manually whenever you need them.

To start a monitor:

1. In the Tree pane, browse to the **Monitors** node.
 - If it is a shared resource monitor, browse to **System > Shared Resources > Monitors**.
 - If it is a partition monitor, browse to **System > Partition > *Partition_Name* > Monitors**.
2. In the List pane, select the monitor you want to start.
3. In the List pane toolbar, click the **Start**  button.