



Enterprise Chat and Email Administrator's Guide to System Console, Release 12.0(1) ES1

For Unified Contact Center Enterprise

First Published: January 11, 2019

Last Updated: August 30, 2019

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<https://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 UCBs 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.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned 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. (1110R)

Enterprise Chat and Email Administrator's Guide to System Console: For Unified Contact Center Enterprise. August 29, 2019

© 2016-2019, Cisco Systems, Inc. All rights reserved.

Contents

- Preface6**
 - About This Guide 7
 - Change History 7
 - Related Documents 7
 - Communications, Services, and Additional Information 8
 - Cisco Bug Search Tool 8
 - Field Alerts and Field Notices 8
 - Documentation Feedback 8
 - Document Conventions 9

- 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 ECE Mail Services 17
 - Setting up ECE Services for Chats 30
 - Setting up Services for Email 30
 - Configuring Additional Workflow Process and Instances 31

- Chapter 3: Business Partition.....32**
 - About the Business Partition. 33
 - Managing the Business Partition. 33

| | |
|--|----|
| Managing Service Instances | 33 |
| Increasing the Number of Service Instances | 33 |
| Removing Service Instances | 34 |
| Viewing Database Details | 35 |
| Assigning Permissions | 36 |

Chapter 4: Managing Hosts38

| | |
|--------------------------|----|
| About Hosts. | 39 |
| Editing Hosts. | 39 |
| Deleting Hosts. | 40 |
| Stopping Hosts | 40 |
| Starting Hosts | 40 |

Chapter 5: Services41

| | |
|---|----|
| About Services, Service Processes, and Service Instances | 42 |
| Services | 42 |
| Unified CCE | 42 |
| Email Services | 43 |
| General Services | 43 |
| Workflow Services | 43 |
| Service Processes | 44 |
| Service Instances | 44 |
| Managing Service Processes | 44 |
| Creating Service Processes | 44 |
| Deleting Service Processes | 45 |
| Increasing the Number of Instances for Service Processes. | 45 |
| Starting Service Processes. | 46 |
| Stopping Service Processes. | 46 |
| Managing Service Instances | 47 |
| Creating Service Instances | 47 |
| Deleting Service Instances | 48 |
| Starting Service Instances | 48 |
| Stopping Service Instances | 49 |
| Adding Aliases to Retriever Instances | 49 |
| Configuring an EAAS Service Instance | 49 |
| Configuring the MR Connection Port for an EAAS Service Instance | 49 |

| | |
|--|-----------|
| Configuring Security Settings for an EAAS Service Instance | 50 |
| Configuring an EAMS Service Instance | 51 |
| Configuring Peripheral Gateway and CTI Server Details | 51 |
| Configuring Security Settings for an EAMS Service Instance | 51 |
| Configuring Context Service for ECE | 53 |
| Chapter 6: Loggers | 55 |
| About Loggers | 56 |
| List of Processes Available in the System | 56 |
| Managing Logging for Processes | 58 |
| Viewing Logging Details for Processes | 58 |
| Changing the Logging Trace Levels for Processes | 59 |
| Enabling Logging for Specific Users | 60 |
| Managing Logging for Process Groups | 61 |
| Configuring Logging for Process Groups | 62 |
| Changing the Logging Trace Levels for Process Groups | 63 |
| Removing Logging for Process Groups | 64 |
| Chapter 7: Monitors | 65 |
| About Monitors | 66 |
| Host Monitors | 66 |
| Service Process Monitors | 66 |
| Service Instance Monitors | 67 |
| Configuring Monitors | 68 |
| Deleting Monitors | 70 |
| Starting Monitors | 70 |

Preface

- ▶ [About This Guide](#)
- ▶ [Change History](#)
- ▶ [Related Documents](#)
- ▶ [Communications, Services, and Additional Information](#)
- ▶ [Field Alerts and Field Notices](#)
- ▶ [Documentation Feedback](#)
- ▶ [Document Conventions](#)

Welcome to the Enterprise Chat and Email (ECE) feature, which provides multichannel interaction software used by businesses all over the world as a core component to the Unified Contact Center Enterprise product line. ECE offers a unified suite of the industry’s best applications for chat and email interaction management to enable a blended agent for handling of web chat, email and voice interactions.

About This Guide

Enterprise Chat and Email 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.

Change History

This table lists changes made to this guide. Most recent changes appear at the top.

| Change | See | Date |
|--|---|--------------|
| Update of Document | | August 2019 |
| Updated information about generating certificates for EAAS and EAMS services | “Configuring Security Settings for an EAAS Service Instance” on page 50 and “Configuring Security Settings for an EAMS Service Instance” on page 51 | |
| Initial Release of Document for Release 12.0(1) | | January 2019 |
| Updated link in Related Documents section to correct URL | “Related Documents” on page 7 | |

Related Documents

The latest versions of all Cisco documentation can be found online at <https://www.cisco.com>

| Subject | Link |
|---|---|
| Complete documentation for Enterprise Chat and Email, for both Cisco Unified Contact Center Enterprise (UCCE) and Cisco Packaged Contact Center Enterprise (PCCE) | https://www.cisco.com/c/en/us/support/contact-center/enterprise-chat-email-12-0-1/model.html |

Communications, Services, and Additional Information

- ▶ To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- ▶ To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- ▶ To submit a service request, visit [Cisco Support](#).
- ▶ To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- ▶ To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- ▶ To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

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 <https://www.cisco.com/cisco/support/notifications.html>

Documentation Feedback

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

We appreciate your comments.

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

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. 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 and can access it through a unique URL: https://ECE_Web_Server/system/web/view/platform/common/login/root.jsp?partitionId=0.

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:** service servers that are part of the installation.
- ▶ **Logger:** loggers 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, for example, 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 and can access it from the partition URL: https://ECE_Web_Server/system/web/view/platform/common/login/root.jsp?partitionId=1

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 services servers are installed and are configured from the System Console for the whole system. An installation can have only one services server.

Loggers

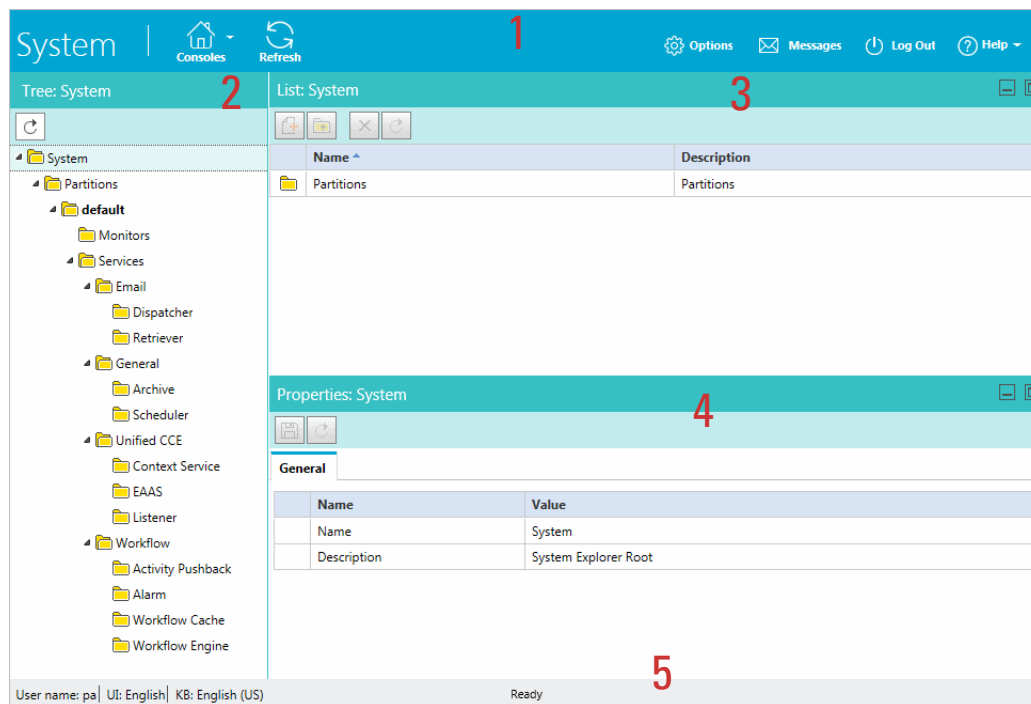
Loggers are used for maintaining and debugging applications. Developers embed various types of trace messages in the code at critical points. These trace messages are logged in appropriate files on client side or server side as per the settings, helping the maintenance engineers trace the cause of a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

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. Plan your requirements before configuring the system accordingly. This would typically include:

- ▶ Managing 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 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 44](#) and [“Managing Service Instances” on page 47](#) for details of the procedures mentioned in this section.

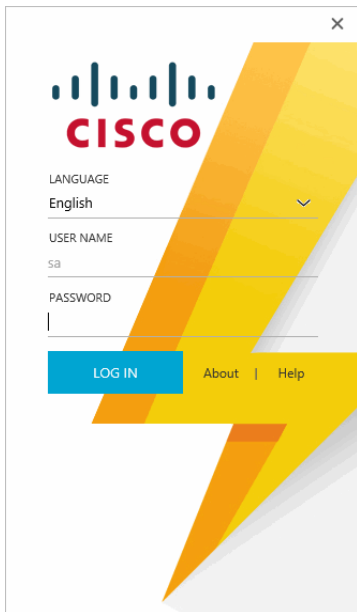
Setting up ECE Mail Services

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.
- ▶ **External Agent Message Service (EAMS):** 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.

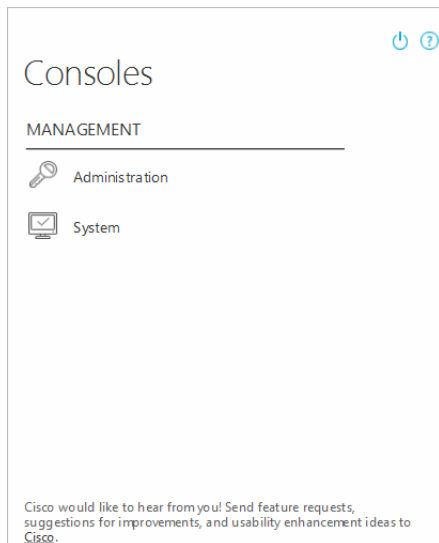
To set up ECE Mail services:

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



Log in as system administrator into system area

2. Go to the System Console.



Select the System Console

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

The screenshot shows the System console interface. On the left, a tree view shows the navigation path: System > Partitions > default > Services > Email > Retriever. The main area is split into two panes. The top pane, titled 'List: Retriever', contains a table with one instance:

| Instance Name | Description | State |
|---------------|--------------------|---------|
| rx-instance | Retriever instance | Running |

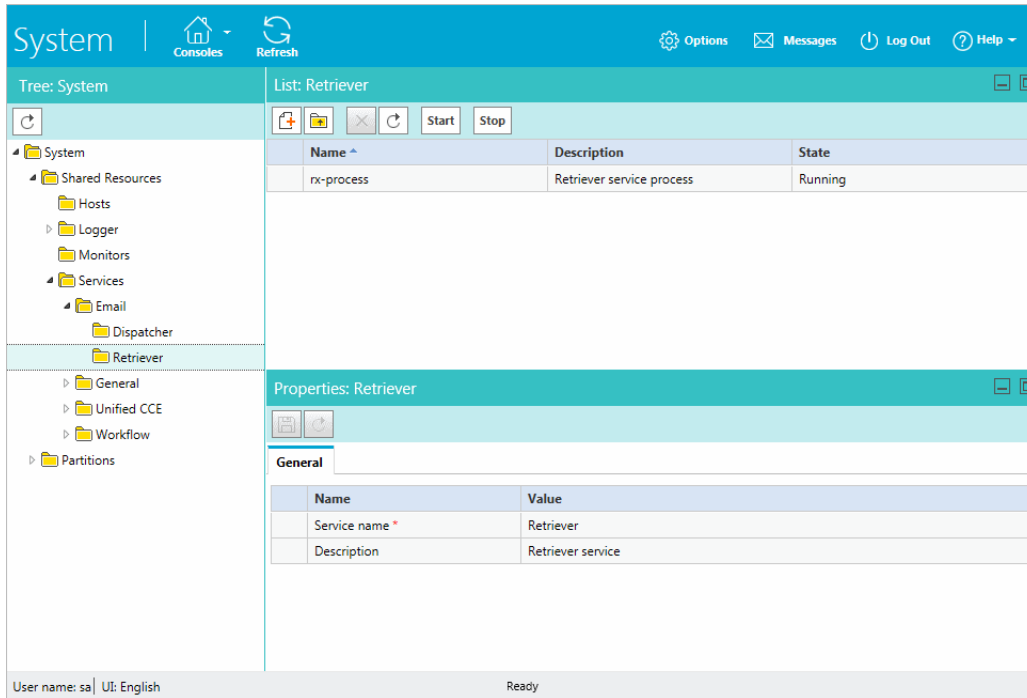
The bottom pane, titled 'Properties: Retriever', shows the 'General' tab with the following details:

| Name | Value |
|----------------|-------------------|
| Service name * | Retriever |
| Description | Retriever service |

At the bottom of the console, the status bar shows 'User name: sa | UI: English' and 'Ready'.

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 Resources > Services > Email > 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** > **Email** > **Retriever** node. Ensure that the start type for the service instance is set to automatic. Stop and start the Retriever instance.

The screenshot shows the System console interface. On the left is a tree view with the following structure:

- System
 - Shared Resources
 - Partitions
 - default
 - Monitors
 - Services
 - Email
 - Dispatcher
 - Retriever
- General
- Unified CCE
- Workflow

The main area is titled "List: Retriever" and contains a table with the following data:

| Instance Name | Description | State |
|---------------|--------------------|---------|
| rx-instance | Retriever instance | Running |

Below the table is the "Properties: rx-instance" section, which has two tabs: "General" and "Input". The "General" tab is active and shows the following configuration:

| Name | Value |
|-----------------|--------------------|
| Instance name * | rx-instance |
| Description | Retriever instance |
| Start type * | Automatic |

At the bottom of the console, the status bar shows "User name: sa | UI: English" on the left and "Ready" on the right.

Start the Retriever instance

- Browse to **Shared Resources > 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 **Start** 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 navigation tree is expanded to 'System > Shared Resources > Services > Workflow > Workflow Cache'. The main area displays a table titled 'List: Workflow Cache' with the following data:

| Name | Description | State |
|---------------------|-----------------------------|---------|
| rules-cache-process | Rules cache manager process | Running |

Below the table, the 'Properties: rules-cache-process' section is visible, showing the 'General' tab with the following configuration:

| Name | Value |
|-------------------------------|-----------------------------|
| Name * | rules-cache-process |
| Description | Rules cache manager process |
| Start type | Automatic |
| Maximum number of instances * | 1 |

At the bottom of the console, the status bar shows 'User name: sa | UI: English' and 'Ready'.

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.

The screenshot shows the System Console interface. On the left, the navigation tree is expanded to 'System > Partitions > default > Services > Workflow > Workflow Cache'. The main area displays a table titled 'List: Workflow Cache' with the following data:

| Instance Name | Description | State |
|-------------------------|-------------------------|---------|
| workflow-cache-instance | Workflow cache instance | Running |

Below the table, the 'Properties: workflow-cache-instance' section is visible, showing the 'General' tab with the following configuration:

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

At the bottom of the console, the status bar shows 'User name: sa | UI: English' and 'Ready'.

Start the workflow cache instance

- Browse to **Shared Resources > 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.

The screenshot shows the 'System' console interface. On the left, a tree view shows the navigation path: System > Shared Resources > Services > Workflow > Workflow Engine. The main area displays a 'List: Workflow Engine' table with one entry:

| Name | Description | State |
|---------------|---------------|---------|
| rules-process | Rules process | Running |

Below the list, the 'Properties: rules-process' window is open, showing the 'General' tab. The properties are as follows:

| Name | Value |
|-------------------------------|---------------|
| Name * | rules-process |
| Description | Rules process |
| Start type | Automatic |
| Maximum number of instances * | 1 |

The status bar at the bottom indicates 'User name: sa | UI: English' and 'Ready'.

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 is a tree view with the following structure:

- System
 - Shared Resources
 - Partitions
 - default
 - Monitors
 - Services
 - Email
 - General
 - Unified CCE
 - Workflow
 - Activity Pushback
 - Alarm
 - Workflow Cache
 - Workflow Engine

The main area displays a list of Workflow Engine instances:

| Instance Name | Description | State |
|-------------------|--------------------------|---------|
| workflow-instance | Workflow engine instance | Running |

Below the list, the properties for the selected 'workflow-instance' are shown in the 'General' tab:

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

At the bottom of the console, the status bar shows: User name: sa | UI: English | Ready

Start the Workflow Engine instance

10. Browse to **Shared Resources > 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 **Start** button. Also ensure that the start type for the service process is set to automatic.

The screenshot displays the System console interface. On the left, a tree view shows the navigation path: System > Shared Resources > Services > Email > Dispatcher. The main area is titled 'List: Dispatcher' and contains a table with the following data:

| Name | Description | State |
|------------|----------------------------|---------|
| dx-process | Dispatcher service process | Running |

Below the list, the 'Properties: dx-process' window is open, showing the 'General' tab. The properties are as follows:

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

The status bar at the bottom indicates 'User name: sa | UI: English' and 'Ready'.

Verify that the Dispatcher process is running

11. 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.

The screenshot displays the System Console interface. On the left, a tree view shows the navigation path: System > Partitions > default > Services > Email > Dispatcher. The main area is titled 'List: Dispatcher' and contains a table with one instance:

| Instance Name | Description | State |
|---------------|---------------------|---------|
| dx-instance | Dispatcher instance | Stopped |

Below the table, the 'Properties: dx-instance' section is visible, showing the 'General' tab with the following configuration:

| Name | Value |
|-----------------|---------------------|
| Instance name * | dx-instance |
| Description | Dispatcher instance |
| Start type * | Automatic |

At the bottom of the console, the status bar shows 'User name: sa | UI: English' and 'Ready'.

Start the Dispatcher instance

12. Browse to **Shared Resources > Services > Unified CCE > EAMS** and verify that the EAMS 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 displays the 'System' console interface. On the left, a tree view shows the navigation path: System > Shared Resources > Services > Unified CCE > EAMS. The main area is divided into two sections: 'List: EAMS' and 'Properties: EAMS-process'.

List: EAMS

| Name | Description | State |
|--------------|--|---------|
| EAMS-process | This process connects to Unified CCE Ag... | Running |
| eams2 | | Stopped |

Properties: EAMS-process

General

| Name | Value |
|-------------------------------|--|
| Name * | EAMS-process |
| Description | This process connects to Unified CCE Agent PG to manage agent states and activities. |
| Start type | Manual |
| Maximum number of instances * | 1 |

User name: sa | UI: English | Ready

Verify that the EAMS process is running

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

The screenshot shows the System Console interface. On the left, a tree view shows the navigation path: System > Partitions > default > Services > Unified CCE > EAMS. The main area displays a list of EAMS instances and the properties for the selected 'AgentNPG' instance.

List: EAMS

| Instance Name | Description | State |
|---------------|--|---------|
| AgentNPG | AgentNPG | Running |
| AgentPG2 | AgentPG2 | Stopped |
| EAMS-instance | This instance connects to Unified CCE A... | Stopped |

Properties: AgentNPG

General | Security

| Name | Value |
|------------------------------|--------------|
| Instance name * | AgentNPG |
| Description | AgentNPG |
| Start type * | Manual |
| Agent PG | AgentNPG |
| Primary CTI Server Address * | 10.10.29.158 |
| Primary CTI Server Port * | 42067 |
| Secondary CTI Server Address | |
| Secondary CTI Server Port | |

User name: sa | UI: English | Ready

Configure EAMS service instance

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

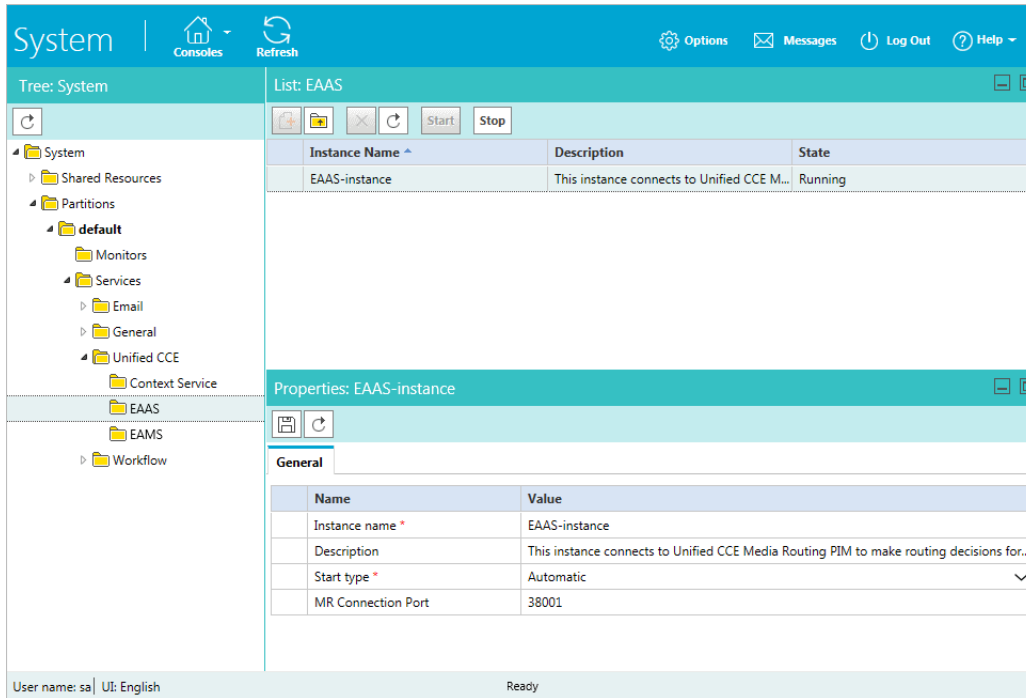
The screenshot shows the 'System' console interface. On the left, a tree view shows the navigation path: System > Shared Resources > Services > Unified CCE > EAAS. The main area displays a list of EAAS processes. One process, 'EAAS-process', is shown with a state of 'Running'. Below the list, the 'Properties: EAAS-process' window is open, showing the 'General' tab. The properties table is as follows:

| Name | Value |
|-------------------------------|--|
| Name * | EAAS-process |
| Description | This process connects to Unified CCE Media Routing PIM to make routing decisions for ... |
| Start type | Automatic |
| Maximum number of instances * | 1 |

At the bottom of the console, the status bar shows 'User name: sa | UI: English' and 'Ready'.

Verify that the EAAS process is running

- Browse to **Partitions** > *partition* > **Services** > **Unified CCE** > **EAAS**. Configure the EAAS service instance by providing the MR Connection port number. Use a port number greater than 2000. Also, ensure that the start type for the instance is set to automatic. Start the EAAS service instance.



Start the EAAS service instance

Setting up ECE Services for Chats

The following services are required for ECE:

- ▶ **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.
- ▶ **External Agent Message Service (EAMS):** 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, follow the instructions in steps 12-15 in [“Setting up ECE Mail Services” on page 17](#).

Setting up Services for Email

The following services are required for 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 ECE Mail Services”](#) on page 17.

Configuring Additional Workflow Process and Instances

To support the following loads, two Workflow processes and Instances need to be configured.

Combination of Email, Chat, and Callback: Support for up to 400 Standardized Concurrent Agents

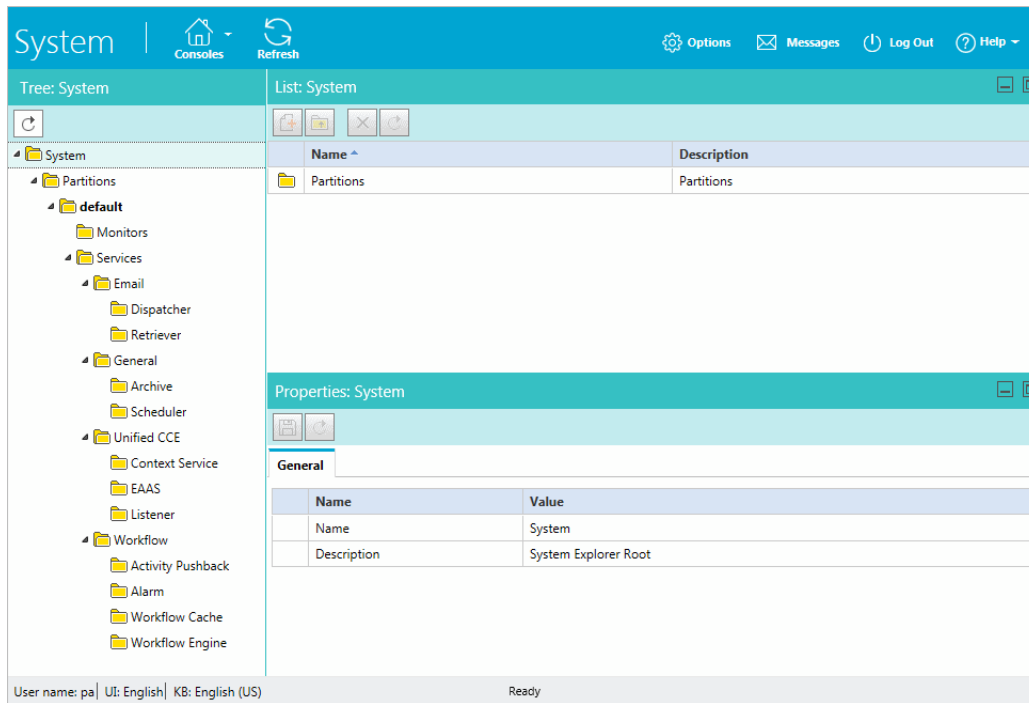
Combination of Email, Chat, and Callback: Support for 401 to 1250 Standardized Concurrent Agents

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.



The System Console while logged in as a partition administrator

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 increase the number of certain service instances to improve performance. You can have more than one service instance for the following services:

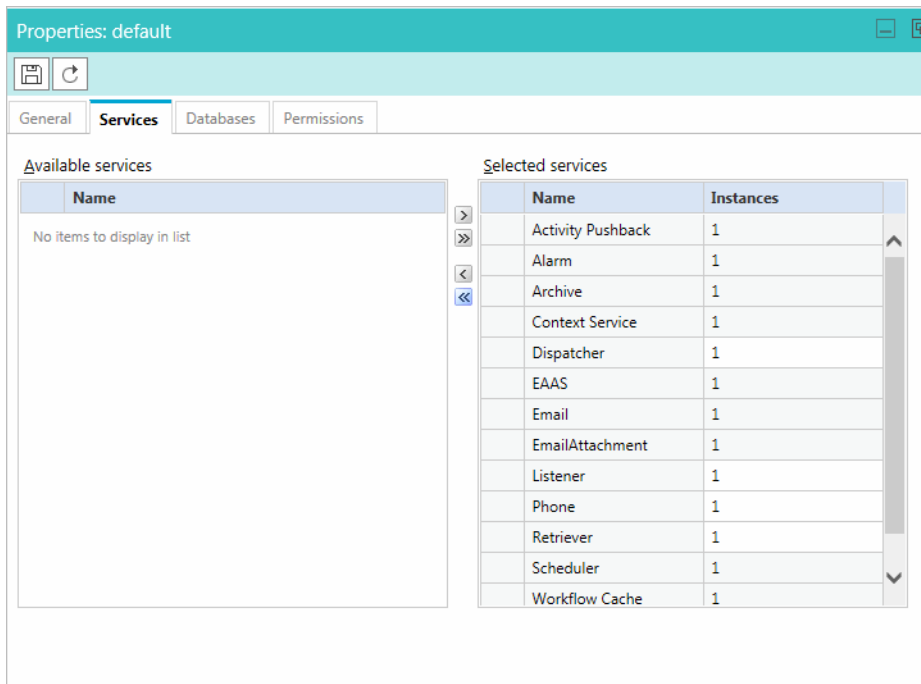
- ▶ Email services: Retriever and Dispatcher

- ▶ Workflow service: Workflow Engine
- ▶ External Agent Message Service (EAMS)

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.

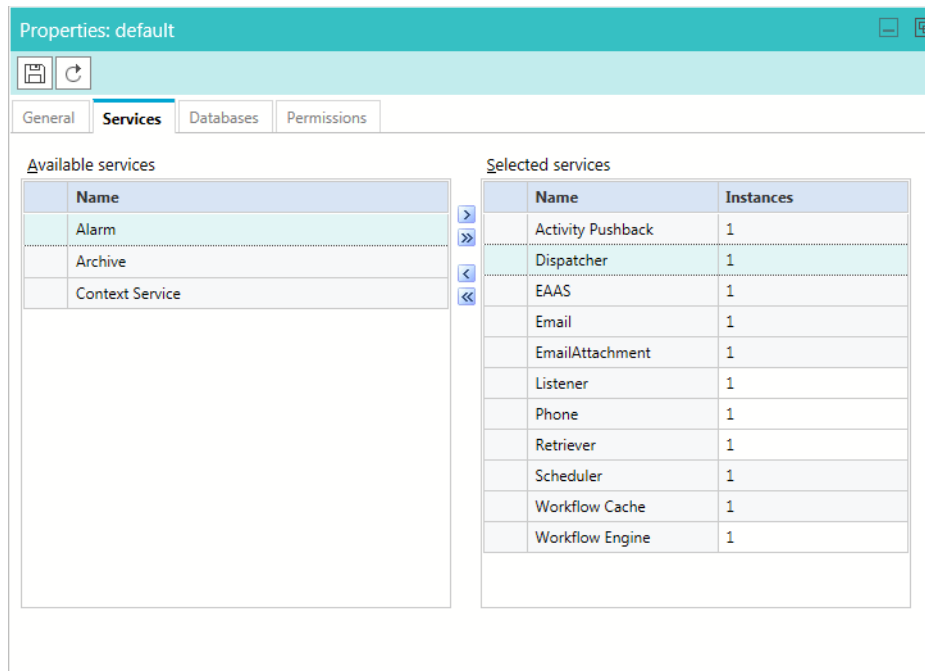
Removing Service Instances

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 Admin Workstation (AW) 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 for the following databases:
 - **Customer DB**
 - **Master DB**
 - **Mail DB**
 - **Archive app DB**
 - **Reports DB**
 - **Author DB**
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**

| customer_db | Name | Value |
|----------------|-------------------|--|
| master_db | Name | Platform_MSSQL_Pool |
| mail_db | Active | Yes |
| archive_app_db | Type | basic |
| reports_db | CapacityIncrement | 2 |
| author_db | InitialCapacity | 1 |
| | MaxCapacity | 600 |
| | DriverName | com.microsoft.sqlserver.jdbc.SQLServerDriver |
| | User | eGActiveDB |
| | Password | ***** |
| | Url | jdbc:sqlserver://ussuhvwm0350:1433;integratedSe... |
| | Targets | |
| | Vendor | mssql |
| | DriverVendor | |

View database details of a partition

Assigning Permissions

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

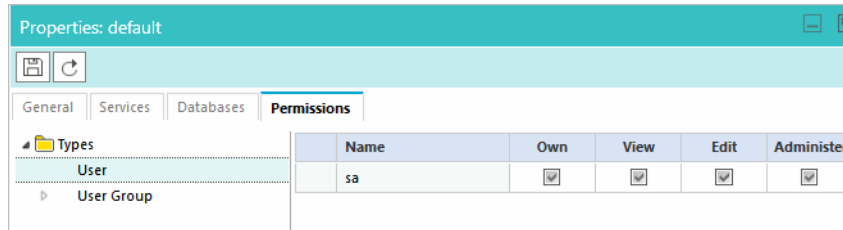
- Own
- View
- Edit
- Administer



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 are managed from the System Console for the overall system. It is the physical machine on which all the services (services server component) for the installation run.

Hosts, that is the services servers, are created during the installation process.

Editing Hosts

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

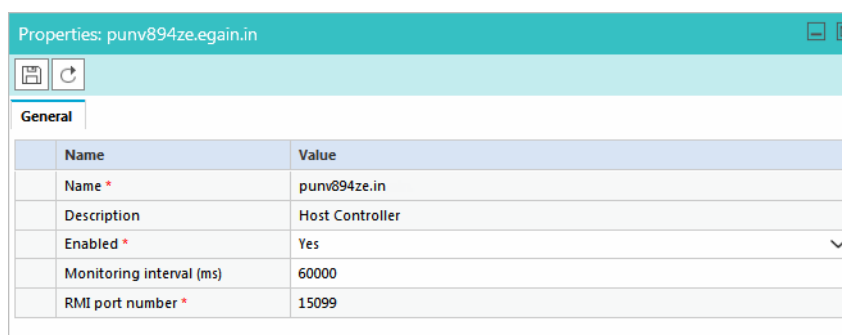
You may want to edit a host property to change its availability in the system. You may also want to monitor the host functions frequently and hence want to change its monitoring interval.

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 cannot be modified. You can only enable or disable the host, or change its monitoring interval. You cannot 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:** Set the value to **Yes** to enable the host. Select **No** to disable the host.
 - **Monitoring interval:** Set the monitoring interval in milliseconds. The default value is 60000 milliseconds.
 - **RMI port number:** The RMI port 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 will not automatically begin running. You have to start 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](#)
- ▶ [Configuring an EAAS Service Instance](#)
- ▶ [Configuring an EAMS Service Instance](#)
- ▶ [Configuring Context Service for ECE](#)

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 the following types:

- ▶ Unified CCE
 - Context Service
 - EAAS
 - EAMS
- ▶ Email services
 - Dispatcher service
 - Retriever service
- ▶ General service
 - Archive (Enterprise) service
 - Report service
 - Scheduler service
- ▶ Workflow services
 - Activity Pushback service
 - Alarm service
 - Workflow Cache service
 - Workflow Engine service

Unified CCE

- ▶ **Context Service:** In addition to the standard services the application comes equipped with the Context Service service. This service allows for the synchronization of specific activity and customer information between the ECE database and the Cisco cloud context service database. The application must be registered and integrated with Unified CCE before the Context Service can be properly configured.

Administrators can use the **Factory Reset** button to reset and reestablish the connection between ECE and Context Service. This may be required when significant updates are made to Context Service. Click this button only when directed to do so by Cisco support. No information is lost from Context Service when you use the factory reset capability.

For more information, see *Enterprise Chat and Email Administrator's Guide to the Administration Console*.

- ▶ **EAAS:** The external agent assignment service (EAAS) routes email, chat, callback, and delayed callback activity 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. If the EAAS service is not running, customers cannot start the chat, callback, and delayed callback sessions and the off hours page is displayed to them. This service can have only one process and instance and neither can be deleted.
- ▶ **EAMS:** The external agent message service (EAMS) 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 agents and tasks to the appropriate Agent PG (i.e. the Agent PG to which the relevant agent belongs). These events are then used by Unified CCE for reporting purposes.

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 (Enterprise) service:** The application uses a partitioning feature provided by the databases to manage growth of high volume objects in active and reports databases. When the application is installed, two partitions are created for the objects in these databases. Groups comprised of multiple partitioning steps are scheduled to run daily, weekly, and monthly. Every time these groups are run, new partitions are added. This ensures that there are always additional partitions available.

A notification email about the success or failure to add a new partition is sent to the email address specified in the partition level setting “To: address for notifications from services”. If a step within group fails, the service attempts to resume the group from same step the next day until it succeeds.

- ▶ **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 consoles. This service can have only one process and instance.
- ▶ **Scheduler service:** This service schedules the messaging and reminder system.

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. These caches are accessed by all rules engine instances before executing rules.
- ▶ **Workflow Engine service:** This service is the main Rules engine. It uses the cache 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.

| Name | Value |
|-----------------------------|------------------------|
| Name * | Sample Service Process |
| Description | |
| Start type | Manual |
| Maximum number of instances | 3 |


Set the general properties

5. 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.
6. 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:

1. In the Tree pane, browse to **System > Shared Resources > Services**.
2. 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.
3. 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
- ▶ External Agent Message Service (EAMS)

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

To increase the number of instances for a service process:

1. In the Tree pane, browse to **System > Shared Resources > Services**.
2. Browse to the service for which you want to increase the number of service instances.
3. 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.
4. 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:

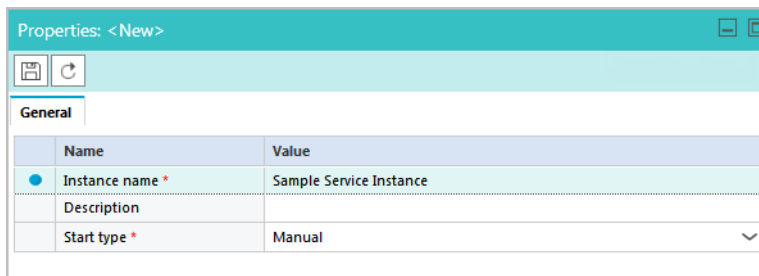
- ▶ Email services: Retriever and Dispatcher
- ▶ Workflow service: Workflow Engine
- ▶ External Agent Message Service (EAMS)

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.



| 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. For more details, see [“Adding Aliases to Retriever Instances” on page 49](#).
6. For the EAAS Service, refer to the following section for more details: [“Configuring an EAAS Service Instance” on page 49](#).

7. For the EAMS, refer to the following section for more details: [“Configuring an EAMS Service Instance” on page 51](#)
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 45.](#)

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 45.](#)
- ▶ Increase the number of instances that can be running in the business partition. For details, see [“Increasing the Number of Service Instances” on page 33.](#)

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, EAMS, Workflow service: Workflow Engine.

Stopping Service Instances

Stop the service instance if it is not needed, freeing up system resources. Changing a server instance's properties may also require a restart of the server instance. 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 an EAAS Service Instance

In addition to the standard fields mentioned in the [“Creating Service Instances” on page 47](#), the EAAS service instance has additional configuration steps to improve the quality and security of the connection.

Configuring the MR Connection Port for an EAAS Service Instance

This is the port used by ECE 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. Use a port number greater than 2000.

Enter this value manually *after* starting ECE, 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 Security Settings for an EAAS Service Instance

The EAAS service instance has security settings that can be configured to protect personally identifiable information that passes through the integrated system.



Important: If the application is integrated with a version prior to Unified CCE 12.0(1), the security settings for EAAS cannot be enabled.

Before configuring security settings for an EAAS service instance, you need to:

- ▶ **Generate a security certificate for the Media Routing servers** that will be used by the instance. A certificate for the primary media routing (MR) server is mandatory and a certificate for the secondary MR server is optional. These certificates are generated and can be obtained in the Cisco Unified CCE environment. For more information, consult *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise*.
- ▶ **Generate a private key in the ECE environment.** To generate a private key:
 - In the ECE environment, open command prompt (`cmd.exe`)
 - Go to the file location: `application_server\ECE_installation_directory\Java\jdk\bin`
 - Execute the command: `keytool -genkey -keyalg RSA -alias ecesaml -keystore ecesaml.jks -validity validity_in_days`
validity_in_days indicates the number of days the certificate should be valid.
 - Provide the necessary details for the security certificate.

This generates the JKS file in the bin folder to be used in the configuration process.

To configure security settings for an EAAS service instance:

1. While configuring an EAAS service instance, in the Properties pane, click the **Security** tab:
 - **Enable Security:** Click the dropdown and select **Yes** to enable or **No** to disable the security configuration.
 - **MR Certificate:** Click the **Assistance** button. In the window that appears, provide the security certificate of the primary Media Routing server.
 - **Secondary MR Certificate:** Click the **Assistance** button. In the window that appears, provide the security certificate of the secondary Media Routing server.
 - **Private Key:** Click the **Assistance** button. In the Private Key window, provide the following details from the private key file that was generated in the ECE environment:
 - **Java keystore file:** Provide the file path of your Java Keystore File. This file will be in .jks format and contains the decryption key the application needs to access files secured by the instance.
 - **Alias name:** The unique identifier for the decryption key.
 - **Keystore password:** The password required for accessing the Java Keystore File.
 - **Key password:** The password required for accessing the Alias' decryption key.

- **Public Key:** Providing the details to Private Key field generates a public key here. Click the **Assistance** button to view the certificate. This certificate must be installed on the Unified CCE environment. For more information about installing the public key on the Unified CCE environment, consult your Cisco Unified CCE documentation.
 - **Supported Cipher Suites:** Provide one or more strings of the desired cipher suite names, separated by colons. The suite names must be in TLS format. For more information about which cipher suite names are accepted, consult your Cisco Unified CCE documentation.
2. After you have configured the required values and saved your changes, you can click the **Test** button to verify your settings are valid and secure. You must restart the service process and instances after saving your changes.

Configuring an EAMS Service Instance

In addition to the standard fields mentioned in the [“Creating Service Instances” on page 47](#), the EAMS service instance has additional configuration steps to improve the quality and security of the connection.

Configuring Peripheral Gateway and CTI Server Details

While configuring an EAMS service instance, under the general tab the following fields are can be configured:

- ▶ **Agent PG:** This is a required field. From the dropdown list, select the Agent PG to which the instance should connect. For auto-configured instances, this field is configured automatically and shows the name of the Agent PG that was selected in the integration wizard.

Below, provide the details of the CTI server in the following fields. For more information about obtaining this information, consult your Cisco Unified CCE documentation.

- ▶ **Primary CTI Server Address:** Provide the IP address of the primary CTI server that is used to handle call activities. This is a required field.
- ▶ **Primary CTI Server Port:** This value is governed by Unified CCE. Provide the value that was provided during the integration process. Values can range from 1 to 65535. This is a required field.
- ▶ **Secondary CTI Server Address:** Provide the IP address of the failover server. This field is not required.
- ▶ **Secondary CTI Server Port:** Provide the port number of the failover server. This field is not required.

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

Configuring Security Settings for an EAMS Service Instance

The EAMS service instance has security settings that can be configured to protect personally identifiable information that passes through the integrated system.



Important: If the application is integrated with a version prior to Unified CCE 12.0(1), the security settings for EAMS cannot be enabled.

Before configuring security settings for an EAMS service instance, you need to:

- ▶ **Generate a security certificate for the CTI servers** that will be used by the instance. A certificate for the primary CTI server is mandatory and a certificate for the secondary CTI server is optional. These certificates are generated and can be obtained in the Cisco Unified CCE environment. For more information, consult your Cisco Unified CCE documentation.
- ▶ **Generate a private key in the ECE environment.** To generate a private key:
 - In the ECE environment, open command prompt (`cmd.exe`)
 - Go to the file location: `application_server\ECE_installation_directory\Java\jdk\bin`
 - Execute the command: `keytool -genkey -keyalg RSA -alias ecesaml -keystore ecesaml.jks -validity validity_in_days`
validity_in_days indicates the number of days the certificate should be valid.
 - Provide the necessary details for the security certificate.

This generates the JKS file in the bin folder to be used in the configuration process.

To configure security settings for an EAMS service instance:

1. While configuring an EAMS service instance, in the Properties pane, click the **Security** tab:
 - **Enable Security:** Click the dropdown and select **Yes** to enable or **No** to disable the security configuration.
 - **CTI Server Certificate:** Click the **Assistance** button. In the window that appears, provide the security certificate of the primary CTI server.
 - **Secondary CTI Server Certificate:** Click the **Assistance** button. In the window that appears, provide the security certificate of the secondary CTI server.
 - **Private Key:** Click the **Assistance** button. In the Private Key window, provide the following details from the private key file that was generated in the ECE environment:
 - **Java keystore file:** Provide the file path of your Java Keystore File. This file will be in .jks format and contains the decryption key the application needs to access files secured by the instance.
 - **Alias name:** The unique identifier for the decryption key.
 - **Keystore password:** The password required for accessing the Java Keystore File.
 - **Key password:** The password required for accessing the Alias' decryption key.
 - **Public Key:** Providing the details to Private Key field generates a public key here. Click the Assistance button to view the certificate. This certificate must be installed on the Unified CCE environment. For more information about installing the public key on the Unified CCE environment, consult your Cisco Unified CCE documentation.
 - **Supported Cipher Suites:** Provide one or more strings of the desired cipher suit names, separated by colons. The suite names must be in TLS format. For more information about which cipher suite names are accepted, consult your Cisco Unified CCE documentation.
2. After you have configured the required values and saved your changes, you can click the **Test** button to verify your settings are valid and secure. You must restart the service process and instances after saving your changes.

Configuring Context Service for ECE



Important: This section only applies to systems using Cisco Context Service.

The ECE application must be registered from Unified CCE or Packaged CCE before the Context Service can be properly configured. The Enterprise Chat and Email Context Service must also be registered with Finesse and Unified CCE or Packaged CCE.

Before you configure and register Context Service, integrate the ECE application with Unified CCE, HCS for Contact Center, or Packaged CCE. The application must be integrated with Unified CCE before the Context Service can be properly configured. For information about integrating the ECE application, see *Enterprise Chat and Email Administrator's Guide to Administration Console*.

| For instructions on how to configure and register Context Service for: | See the Context Service section in: |
|--|---|
| Unified CCE solutions | Cisco Unified Contact Center Enterprise Features Guide |
| Packaged CCE solutions | Cisco Packaged Contact Center Enterprise Features Guide |
| HCS for Contact Center solutions | Configuring Guide Cisco HCS for Contact Center |

To configure the Context Service:

1. Log in as the system administrator and go to the System Console.
2. In the Tree pane, browse to **System > Shared Resources > Services > Unified CCE > Context Service**.
3. In the List pane, select the **Context Service** process.
4. In the Properties pane, adjust the following if necessary:
 - **Proxy Server URL:** When the ECE Services Server or the ECE All-In-One server (in PCCE installations) is behind a firewall and does not have direct access to the internet, a proxyURL should be provided so the server can connect to Cisco Context Service. The URL should be in the format `http://ProxyServerName:Port` or `https://ProxyServerName:Port`
5. Click the **Start** button.



Important: The Context Service process must be running before the instance can be properly configured.

6. In the Tree pane, browse to **System > Partition > *Partition Name* > Services > Unified CCE > Context Service**.
7. In the List pane, select the **Context Service** instance.
8. In the Properties pane, adjust the following if necessary:
 - **Name:** Name of the Instance.
 - **Description:** Description of the Instance.
 - **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.

9. In the List pane, click the **Start** button.



Important: Once Context Service is configured and running in ECE, if Context Service is modified on the Unified or Packaged CCE environment, the Context Service instance must be restarted.

6 Loggers

- ▶ [About Loggers](#)
- ▶ [Managing Logging for Processes](#)
- ▶ [Managing Logging for Process Groups](#)

About Loggers

Logging is a mechanism for capturing log messages as they are encountered while the product is running. For all the java processes running in the system, separate log files are created and messages are logged in these individual files. In a single server installation, all the log files are created on the file server. In distributed server installations, log files for the application server, messaging server, and services server are created on each of these servers and not on the file server.

A list of these processes, along with the log file names, is displayed in the System Console. From the UI, you can change the level of logging, and can filter the log messages for a particular user. Also, you can create a group of processes and log all the messages in a single log file to get a comprehensive view of a single functionality, such as a single log file for email, which includes log messages for retriever, dispatcher, and workflow processes.

Messages are logged at eight 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.
- ▶ **8 - Trace:** This log level identifies all the Java methods called during the complete flow of the code. This is the highest level of logging and produces maximum number of log messages.

List of Processes Available in the System

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

| # | Component | Process name | Log file name |
|----|------------------------------------|--|---|
| 1. | Installation program | <i>Server_Name</i> : eGainInstaller | eg_log_ <i>Server_Name</i> _eGainInstaller.log |
| 2. | Updater | <i>Server_Name</i> : upgrade-installer | eg_log_ <i>Server_Name</i> _upgrade-installer.log |
| 3. | Deployment Configuration Utility | <i>Server_Name</i> : eGConfigUtility | eg_log_ <i>Server_Name</i> _eGConfigUtility.log |
| 4. | Distributed Services Manager (DSM) | <i>Services_Server_Name</i> : DSMController | eg_log_ <i>Services_Server_Name</i> _DSMController.log |
| 5. | Distributed Services Manager (DSM) | <i>Services_Server_Name</i> : dsm-registry | eg_log_ <i>Services_Server_Name</i> _dsm-registry.log |
| 6. | Distributed Services Manager (DSM) | <i>Services_Server_Name</i> : HostController | eg_log_ <i>Services_Server_Name</i> _HostController.log |

| # | Component | Process name | Log file name |
|-----|------------------------------------|---|--|
| 7. | Distributed Services Manager (DSM) | <i>Services_Server_Name:</i> ServerMonitoring | eg_log_ <i>Services_Server_Name</i> _ServerMonitoring.log |
| 8. | Distributed Services Manager (DSM) | <i>Services_Server_Name:</i> ServiceController | eg_log_ <i>Services_Server_Name</i> _ServiceController.log |
| 9. | Application server | <i>Application_Server_Name:</i> Application Server | eg_log_ <i>Application_Server_Name</i> _ApplicationServer.log |
| 10. | Agent Assignment service process | <i>Services_Server_Name:</i> agent-assignment-process | eg_log_ <i>Services_Server_Name</i> _agent-assignment-process.log |
| 11. | Alarm service process | <i>Services_Server_Name:</i> alarm-rules-process | eg_log_ <i>Services_Server_Name</i> _alarm-rules-process.log |
| 12. | Archive service process | <i>Services_Server_Name:</i> archive-enterprise-process | eg_log_ <i>Services_Server_Name</i> _archive-process.log |
| 13. | Activity Pushback service process | <i>Services_Server_Name:</i> auto-pushback-process | eg_log_ <i>Services_Server_Name</i> _auto-pushback-process.log |
| 14. | Dispatcher service process | <i>Services_Server_Name:</i> dx-process | eg_log_ <i>Services_Server_Name</i> _dx-process.log |
| 15. | KB Import service process | <i>Services_Server_Name:</i> import-process | eg_log_ <i>Services_Server_Name</i> _import-process.log |
| 16. | Article Rating service process | <i>Services_Server_Name:</i> kb-article-rating-process | eg_log_ <i>Services_Server_Name</i> _kb-article-rating-process.log |
| 17. | Attachment service process | <i>Services_Server_Name:</i> kb-attachments | eg_log_ <i>Services_Server_Name</i> _kb-attachments.log |
| 18. | Report service process | <i>Services_Server_Name:</i> report-process | eg_log_ <i>Services_Server_Name</i> _report-process.log |
| 19. | Workflow Cache service process | <i>Services_Server_Name:</i> rules-cache-process | eg_log_ <i>Services_Server_Name</i> _rules-cache-process.log |
| 20. | Workflow Engine service process | <i>Services_Server_Name:</i> rules-process | eg_log_ <i>Services_Server_Name</i> _rules-process.log |
| 21. | Retriever service process | <i>Services_Server_Name:</i> rx-process | eg_log_ <i>Services_Server_Name</i> _rx-process.log |
| 22. | Scheduler service process | <i>Services_Server_Name:</i> scheduler-process | eg_log_ <i>Services_Server_Name</i> _scheduler-process.log |
| 23. | Context Service process | <i>Services_Server_Name:</i> ContextService-process | eg_log_ <i>Services_Server_Name</i> _ContextService-process.log |
| 24. | EAAS service process | <i>Services_Server_Name:</i> EAAS-process | eg_log_ <i>Services_Server_Name</i> _EAAS-process.log |
| 25. | EAMS service process | <i>Services_Server_Name:</i> EAMS-process | eg_log_ <i>Services_Server_Name</i> _EAMS-process.log |

Managing Logging for Processes

When a Java process is started in the system, an entry is automatically created in the System Console that displays the logger information for that process such as the log file name, trace level, etc.

The system allows you to change the log trace levels for these process and to create filters to enable logging for specific users. You cannot create new loggers or delete existing ones.



Important: All the changes described in this section take affect immediately. You do not need to restart anything after making these changes.

Viewing Logging Details for Processes

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

To view the properties of a process logger:

1. In the Tree pane, browse to **System > Shared Resources > Logger > Processes**.
2. In the List pane, select a process.
3. In the Properties pane, you can view the following details of the logger.
 - **Name:** The name of the logger.
 - **Description:** The description of the logger.
 - **Log file name:** The name of the log file in which the log messages are recorded.
 - **Maximum File Size:** The maximum size of the log file. The value is set to 5 MB.
 - **Maximum trace level:** The maximum level of logging done by the logger. For more details, see [“Changing the Logging Trace Levels for Processes” on page 59](#).
 - **User ID, HTTP session ID:** You can also create a filter to record messages for a particular user, or a session of the user. For details see, [“Enabling Logging for Specific Users” on page 60](#).

| Name | Value |
|----------------------------|--|
| Name | punv894ze:alarm-rules-process |
| Description | punv894ze:alarm-rules-process |
| Maximum trace level | 2 - Error |
| Log file name | eg_log_punv894ze_alarm-rules-process.log |
| Maximum file size | 5MB |
| Extensive logging duration | <Select> |
| Extensive logging end time | |

View the general properties

Changing the Logging Trace Levels for Processes

You can edit process loggers only if the “Edit Handler” 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.

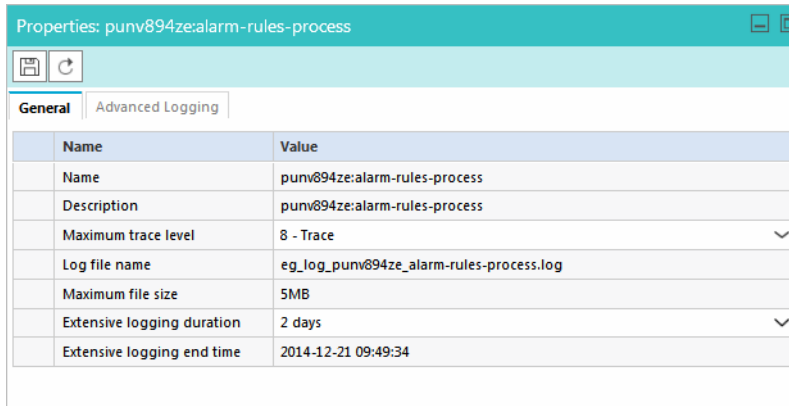
To change the logging trace levels for a process:

1. In the Tree pane, browse to **System > Shared Resources > Logger > Processes**.
2. In the List pane, select the process 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.
 - **8 - Trace:** This level provides tracing information at the Java API level. 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. Since **Debug** and **Trace** are extensive logging levels, you need to set a time at which the logging should end at these levels. Once the logging ends, the maximum trace level is reset to the trace level that was set prior to the **Debug** or **Trace** level. In the Extensive logging duration field, In the **Extensive logging duration** field, select one of the following:
 - 10 minutes
 - 30 minutes
 - 1 hour
 - 2 hours
 - 4 hours
 - 1 day
 - 2 days
 - 1 week

The **Extensive logging end time** field automatically displays the time when the extensive logging for the process will end.



| Name | Value |
|----------------------------|--|
| Name | punv894ze:alarm-rules-process |
| Description | punv894ze:alarm-rules-process |
| Maximum trace level | 8 - Trace |
| Log file name | eg_log_punv894ze_alarm-rules-process.log |
| Maximum file size | 5MB |
| Extensive logging duration | 2 days |
| Extensive logging end time | 2014-12-21 09:49:34 |

Set the trace level for the process

5. Click the **Save**  button.

Enabling Logging for Specific Users

You can configure a process logger to log messages for a specific user or for a specific session of a user. This lets you troubleshoot issues with a specific user or a particular session of a user. This feature should be used very selectively as when logging is being done for only one user, or only a particular session of a user, the logging for the rest of the users does not happen during that time.

To get started, you need to first get the user ID and HTTP session ID of the user from the database.

- ▶ To get the user ID, run the following query on the active database:

```
Select user_ID from egpl_user where user_name = User_Name
```

Where *User_Name* is the name of the user you want to monitor.

- ▶ To get the HTTP session ID, run the following query on the active database:

```
Select session_ID from egpl_user_session_details  
where user_ID in (select user_ID from egpl_user where user_name = 'User_Name')  
and server_key in (select pkey from egpl_server_status where server_name =  
'Application_Server_Name')
```

Where *User_Name* is the name of the user you want to monitor, and *Application_Server_Name* is the name of the application server from where the user is logged in.

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

To enable logging for a specific user:

1. In the Tree pane, browse to **System > Shared Resources > Logger > Processes**.
2. In the List pane, select the process you want to edit.
3. In the Properties pane, click the Advanced Logging tab.

4. Enable and set the following and specify the trace level and extensive logging durations (page 59):



Important: Package and Class are advanced features and should be used only under the guidance of Cisco TAC.

- **User ID:** Provide the ID of the user for which you want to log messages. Only one user ID can be provided at a time.
- **HTTP session ID:** Provide the HTTP session ID of the user for which you want to log messages. Only one session ID can be provided at a time.

Ensure that the values in these fields are correct. If the user ID and HTTP session ID do not match, no logs are created.

| User | Name | Value |
|--------------|---------------------------|---------------------------------|
| HTTP Session | Enable advanced log... | Yes |
| Package | HTTP Session IDs (com... | 1620E6E95EJRNT6JGO55FKR44433FGG |
| Class | Maximum trace level | 4 - Info |
| | Extensive logging dur... | <Select> |
| | Extensive logging en... | |
| | Log file name | |
| | Maximum log file size ... | |

Set logging for a specific user or user session

5. Click the **Save** button.

After troubleshooting is complete, remove the user ID and session ID from here to reset regular logging for the process.

Managing Logging for Process Groups

Process groups can be created to capture comprehensive logging for a particular functionality. For example, if you want to record all the messages related to email infrastructure in a single log file, you can create a process group that includes retriever, dispatcher, workflow engine processes. Instead of looking at three log files, you can now get all the messages in a single log file. A different logging level can also be configured for these processes at the group level.

When a process is included in a process group, the logging for the process continues in the process log file. Additional logging for the process is also done in the process group log file at the trace level configured for the process group.

In a distributed-server installation, if a process group includes the components that are installed on different machines, then separate process group log files will be generated on each server and will capture the information about only the components that are installed on that particular machine. For example, if you create a process group with processes ApplicationServer, retriever, and workflow and the application server and services server

are installed on two different machines, then a log file for the same process group will be created on each server. On the application server, it will contain logging data of the ApplicationServer process and on the services server, it will contain logging data of retriever and workflow processes.


You need the “View Logger” (to view, create, and delete) and “Edit Logger” (to edit, view, create, and delete) actions to manage process groups.

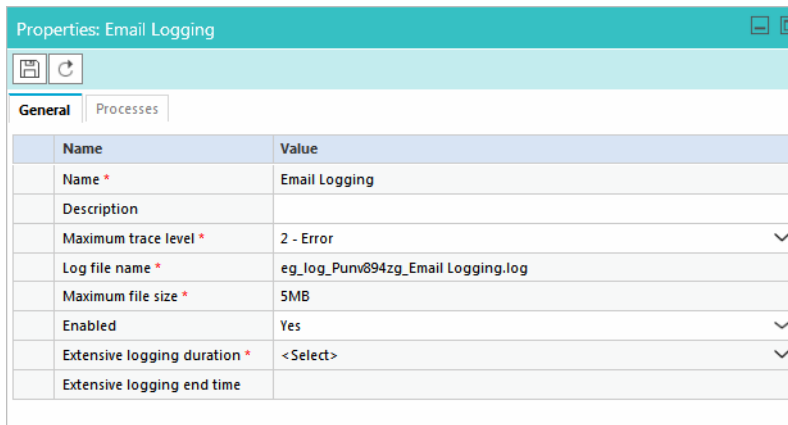


Important: All the changes described in this section take affect immediately. You do not need to restart anything after making these changes.

Configuring Logging for Process Groups

To configure logging for process groups:

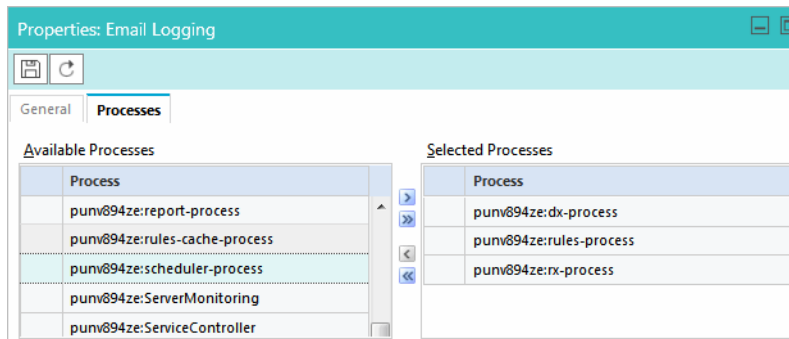
1. In the Tree pane, browse to **System > Shared Resources > Logger > Process Groups**.
2. In the List pane toolbar, click the **New**  button.
3. In the Properties pane, on the General tab, provide the following details.
 - **Name:** The name of the process group.
 - **Description:** Provide a brief description.
 - **Maximum trace level:** The maximum level of logging done by the process group. For more details, see [“Changing the Logging Trace Levels for Process Groups” on page 63](#).
 - **Log file name:** The name of the log file in which the process group records the log messages. The value in this field is set automatically and it cannot be changed. The format of the log file name is `eg_log_Process_Group_Name.log`.
 - **Maximum File Size:** The maximum size of the log file. The value is set to 5 MB. The value in this field is set automatically and it cannot be changed.
 - **Enabled:** Select **Yes** to enable logging.



| Name | Value |
|------------------------------|------------------------------------|
| Name * | Email Logging |
| Description | |
| Maximum trace level * | 2 - Error |
| Log file name * | eg_log_Punv894zg_Email Logging.log |
| Maximum file size * | 5MB |
| Enabled | Yes |
| Extensive logging duration * | <Select> |
| Extensive logging end time | |

View the general properties

- In the Properties pane, on the Processes tab, select the process to be included in the process group.



Select the processes

- Click the **Save**  button.

Changing the Logging Trace Levels for Process Groups

You can change the trace level of process groups if the “View Logger” (to view, create, and delete) and “Edit Logger” (to edit, view, create, and delete) 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:

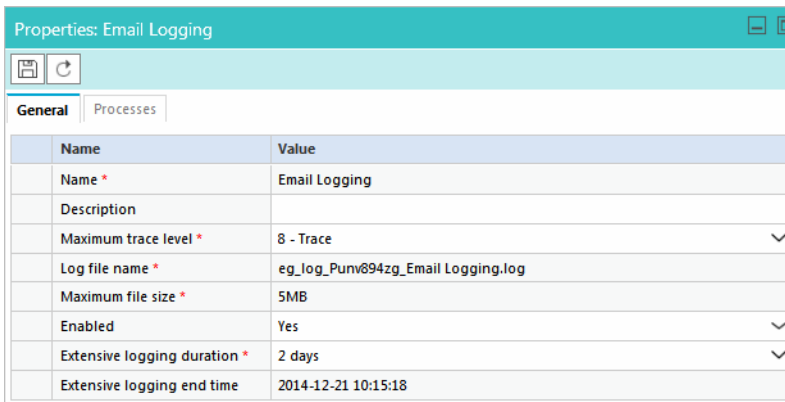
- In the Tree pane, browse to **System > Shared Resources > Logger > Process Groups**.
- In the List pane, select the process group you want to edit.
- In the Properties pane, change the value in the **Maximum trace level** field. The options available are:
 - 1 - Fatal:** This level identifies critical 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.
 - 8 - Trace:** This log level identifies all the Java methods called during 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.

- Since **Debug** and **Trace** are extensive logging levels, use them only for limited periods of time. Once the logging ends, the maximum trace level is reset to the trace level that was set prior to the **Debug** or **Trace** level. In the **Extensive logging duration** field, select one of the following:

- 10 minutes
- 30 minutes
- 1 hour
- 2 hours
- 4 hours
- 1 day
- 2 days
- 1 week

The **Extensive logging end time** field automatically displays the time when the extensive logging for the process is set to end.





Set the trace level

5. Click the **Save**  button.

Removing Logging for Process Groups

After you are done logging for process groups, you can either disable the process group logging, or you can delete it.

To remove logging for process groups:

1. In the Tree pane, browse to **System > Shared Resources > Logger > Process Groups**.
2. In the List pane, select the process group for which you want to stop logging. Do one of the following:
 - In the List pane toolbar, click the **Delete**  button. When the process group is deleted, the log file associated with it is not deleted automatically. You need to go to the server machine to delete the file.
 - If you want to keep the process group for future use, then in the Properties pane, in the **Enabled** field select **No**. The process group logging will be disabled.
3. 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, for example, the hosts, service processes, or service instances, and the attributes of the objects to be monitored. 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
- ▶ *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 emails.
- ▶ **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 which the alias is associated.
- ▶ **State**
- ▶ **Throughput**
- ▶ **Pending**
- ▶ **Last Run**
- ▶ **Emails Skipped**

Configuring Monitors

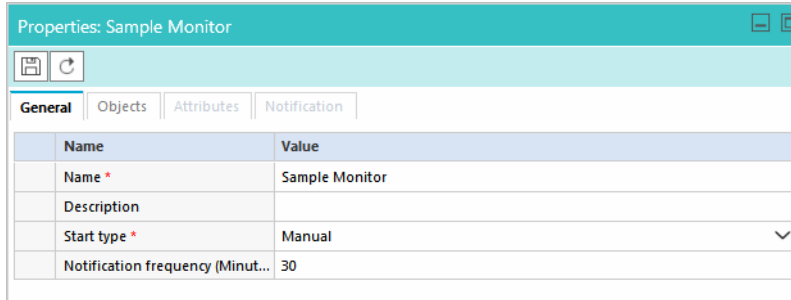
Create different monitors to enable periodic checks on the system resources and business partition resources. These monitors help you keep an account of which system resource is running. Configure monitors such that only the required attributes are displayed in results.

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:

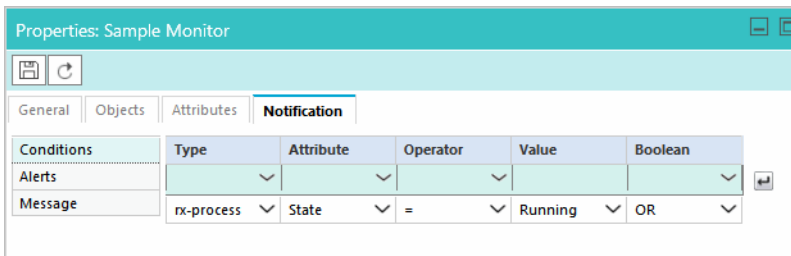
1. In the Tree pane, browse to the **Monitors** node.
 - If it is a shared resource monitor, browse to **System > Shared Resources > Monitors**.
 - If it is a partition monitor, browse to **System > Partition > *Partition_Name* > Monitors**.
2. In the List pane toolbar, click the **New**  button.

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**
 - **Notification frequency (Minutes):** Specify the time interval at which notifications should be sent when a condition specified in the monitor is met. The default value is set to 30 minutes.



Set the general properties

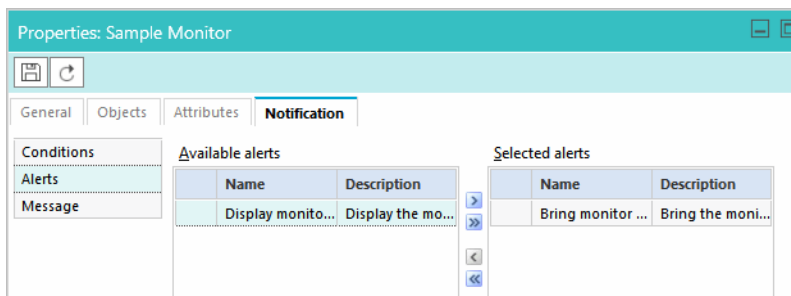
4. Next, go to the Objects tab and select the object to be monitored.
 - For shared resources monitors, select from the list of available hosts and service processes.
 - And, for partition resources, select from the list of available service instances.
 5. Next, go to the Attributes tab and select the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

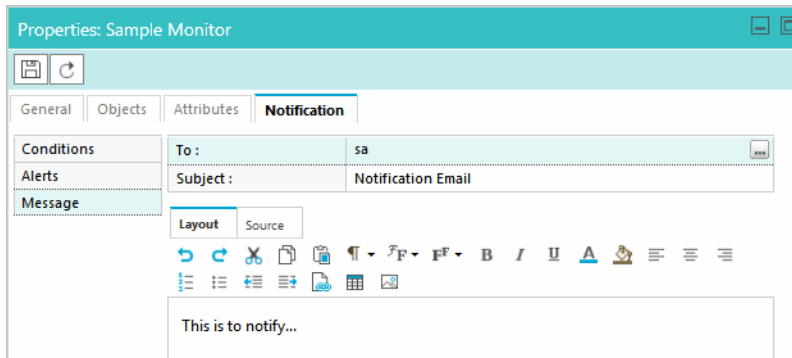


Select alert types

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. In the List pane toolbar, click the **Start** button.