



Cisco Interaction Manager System Console User's Guide

Release 4.1(1)
January 2007

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100



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

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

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

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

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

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

Cisco Interaction Manager System Console User's Guide
© 2007 Cisco Systems, Inc. All rights reserved.

Contents

Preface	6
About this guide	7
Document conventions	7
Other learning resources	8
Online help	8
Document set.	8
Chapter 1: Console basics	9
Key terms and concepts	10
Partitions	10
System administrator.	10
System administrator view	10
Partition administrator.	10
Partition administrator view	11
Shared resources	11
Partition resources.	11
Services	11
Service processes	11
Service instances.	11
Hosts	12
Loggers	12
Monitors	12
Elements of the user interface.	12
Chapter 2: Setting up the system	15
Role of a system administrator	16
Identifying your system requirements	16
Managing resources across the system	16
Managing resources within individual partitions	17
Setting up hosts.	17

Setting up partitions	18
Chapter 3: Managing partitions.....	19
About partitions	20
Adding partitions	20
Editing partitions.	21
Disabling partitions.	22
Chapter 4: Managing hosts	23
About hosts	24
Editing hosts	24
Deleting hosts	25
Chapter 5: Managing services.....	26
About services.	27
Chat	27
Content Index	27
Email	27
General	28
Knowledge Base (KB)	28
Workflow	28
About service processes	29
About service instances	29
Managing service processes	29
Creating service processes	29
Starting service processes	31
Stopping service processes	31
Managing service instances	32
Creating service instances.	32
Starting service instances	33
Stopping service instances	33
Deleting service instances.	33

Chapter 6: Managing loggers35

- About loggers 36
- Configuring loggers 36
- Editing loggers 37
- Working with handlers for shared resources 38
 - About handlers 38
 - Creating handlers 38
- Using filters for shared resources 39
 - About filters 39
 - Creating filters. 39
- Working with logs 40
 - Customizing log displays 40
 - Deleting log reports. 41
- Viewing logs. 41
 - System logs 41
 - Application logs 41

Chapter 7: Monitoring the system43

- About monitors 44
- Configuring monitors 44
- Monitoring hosts 45
 - Starting host monitors 45
 - Stopping host monitors 45
- Monitoring services 46
 - Monitoring service processes 46
 - Monitoring service instances 46
- Deleting monitors 47

Preface

- ▶ [About this guide](#)
- ▶ [Document conventions](#)
- ▶ [Other learning resources](#)

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

About this guide

Cisco Interaction Manager System Console User’s Guide introduces you to the System Console and helps you understand how to use it to accomplish your system setup, monitoring, and troubleshooting tasks.

Document conventions

This guide uses the following typographical conventions.


Convention	Indicates
<i>Italic</i>	Emphasis, or the title of a published document.
Bold	The label of an item in the user interface, such as a field, button, or tab.
Monospace	A file name or command. Also, text that must be typed by the user.
<i>Variable</i>	User-specific text, which is supplied by the user.

Other learning resources

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

Online help

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

Use	To view
 Help button	All topics in <i>Cisco Interaction Manager Help</i> ; the Help button appears in the console toolbar on every screen, as well as on most windows.
F1 keypad button	Context-sensitive information about the item selected on the screen.

Document set

For more information about Cisco Interaction Manager, see the following documents. They can be found in the **Documents** folder on the product CD.

- ▶ *Cisco Interaction Manager System Requirements*
- ▶ *Cisco Interaction Manager Installation Guide*
- ▶ Other Cisco Interaction Manager user's guides

1

Console basics

- ▶ [Key terms and concepts](#)
- ▶ [Elements of the user interface](#)

A highly specialized workspace for system administrators, this console lets you set up and manage the system resources needed for the installation.

Key terms and concepts

Partitions

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

System administrator

System administrators perform technical administration functions to manage the system. They have jurisdiction across partitions. Using the tools provided to them they can monitor various components of the application and also enable or disable partitions. They can specify limits on resources that partitions can use so that one partition cannot overuse resources in the system at the expense of other partitions.

The installation program creates the first system administrator by prompting the user running the install program to enter user id and password information. The system administrator can then log in and create additional peer system administrators using the user creation screens in the application.

System administrator view

The system administrator has a holistic view of the System Console through a unique URL. This URL is especially accessed by the system administrator only. The Shared Resources and Partition nodes are displayed in the console. This user can configure services or hosts for installation and distribute the same across multiple partitions. Each partition then has its own administrator who organizes tasks within it.

Partition administrator

Partition administrators can create new departments and set up the first users within department so that department level users can further set up their system based on their business needs. They have jurisdiction across departments. Partition administrators have the capabilities to set up sharing permissions across departments to enable users from one department to work with another department.

The installation program creates the first partition administrator by prompting the user running the install program to enter user id and password information. The 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 limited view of the System Console from the partition URL. The tree displays only the Partition nodes and sub-nodes within it. The Shared Resources node is not visible to the partition administrator due to lack of permissions.

Shared resources

System administrators work with shared resources to enable services, processes, and hosts across all partitions.

Partition resources

These are specific to individual partitions. They consist of logs, monitors, and service instances. Partition administrator works with the partition resources.

Services

Services accomplish a specialized function. For example, a Dispatcher service is responsible for sending out emails from the system. Similarly other services perform other functions for the system.

Service processes

Service processes work across more than one department, thus minimizing the system load. This uses fewer resources on the server and maximizes the efficiency of the system. For example, one Dispatcher service process could serve one or more deployments. 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 each customer deployment in the system, to accomplish specific

functions. These instances are specific to a deployment and do not work across more than one deployments.

Hosts

Hosts are configured from the System Console for the whole system. These are the physical machines on which the software processes will be running. A host can serve multiple partitions.

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 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:

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 presents the knowledge base folders as a tree list, allowing you to select the node (folder) that you wish to work in. When you select a folder, its first-level contents—subfolders and articles—are displayed in the **List** pane. In the **Tree** pane, you can cut paste or copy paste folders, delete folders which you have created, manage bookmarks and print folder contents.

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 folder or article 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).

2 Setting up the system

- ▶ [Role of a system administrator](#)
- ▶ [Identifying your system requirements](#)
- ▶ [Setting up hosts](#)
- ▶ [Setting up partitions](#)

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 all partitions. You can also enable or disable partitions. Using the tools provided within consoles you work in, monitor various components of the application. Specify limits on resources that partitions use so that partitions cannot overuse resources.

The installation program creates the first system administrator by prompting for user id and password information during installation. Use this id to log in and create additional peer system administrators from the user creation screens in the application.

Identifying your system requirements

Once the installation is through, it becomes your primary responsibility, as a system administrator, to set up the system in an effective manner for your business needs. You might need to plan out your requirements before configuring the system accordingly. This would typically include:

- ▶ Accessing the number of partitions required
- ▶ User-friendly partition names (virtual directories for web servers).
- ▶ Creating hosts and service processes across partitions
- ▶ Creating service instances within each 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

Since you have jurisdiction across all partitions, you will be working with shared resources quite often. Shared resources help you enable services, processes, and hosts across all partitions. In this manner you will not have to administer common tasks for individual partitions one after another. By managing shared resources, you not only cut down on your effort but also enhance consistency.

Any modifications you make under the shared resources node are applicable to all partitions.

The following folders are available within shared resources:

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

Managing resources within individual partitions

System administrators as well as partition administrators work with partition resources to enable services, instances, and monitors specific to particular partitions. As an administrator you can only work with the partitions that you have access permissions to.

At the outset, the installation program creates a default partition. Once the system is configured you can create additional partitions and partition administrators by installing the system repeatedly.

The modifications you make under partition resources node are applicable to only that specific partition.

The following folders are available under each partition:

- ▶ **Loggers:** You can create loggers and log reports for partitions. The log reports here will cater only to the partition for which you have logged the information.
- ▶ **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 this particular partition.

Setting up hosts

Hosts are physical machines on which the system is set up. You can configure each host machine to serve multiple partitions. The number of hosts that you set up for the system will depend on your user base and customer base.

Ensure that your host machines comply with the prerequisites mentioned in *Cisco Interaction Manager Installation Guide*. For detailed information, refer to chapter, "Hosts."

Setting up partitions

Partitions support multiple customer databases on a single product installation. These contain all the business information for one business unit or client. Use partitions to allow physical separation of data to ensure privacy of information. This will also help you maintain independence of different business entities.

You would typically use separate partitions to serve distinct business units or clients. Thus partitions catering to separate entities would not share any data amongst themselves. As a system administrator, you can allot system resources to all partitions from your System Console view. This does not affect the privacy of information.

The installation program creates the default first partition. Create additional partitions by using the Custom Install Option in the installation program. For details, refer to *Cisco Interaction Manager Installation Guide*.

Managing partitions

- ▶ [About partitions](#)
- ▶ [Adding partitions](#)
- ▶ [Editing partitions](#)
- ▶ [Disabling partitions](#)

About partitions

Partitions in a system contain all the information for one business unit or client. Use partitions to allow physical separation of data and ensure privacy of information for different business entities. You can configure multiple partitions on a single system.

Set up partitions such that each serves independent business units. These units may have no need to share customer information or knowledge base data because they may serve different customers. For example a bank that provides services to retail consumers and corporate customers can use multiple partitions since the nature of product offering and customer service needs are different.

Create multiple partitions if you need to segregate your database into mutually exclusive business units. Multiple partitions can either serve different businesses or different units of the same business.

You would typically use separate partitions to serve distinct business units or clients. Thus partitions catering to separate entities would not share any data amongst themselves. As a system administrator, you can allot system resources to all partitions from your System Console view. This does not affect the privacy of information.

The installation program creates the default first partition. It generates two URLs for accessing the Unified System view and the partition view. Unified System view and the partition view have separate users.

Adding partitions

Before setting up your system, plan out your requirements in a thorough fashion. Once you know your requirements, you can create the corresponding number of partitions.

When a new system is installed the installation program creates the first or default partition. To create additional partitions use the Custom Install option of the installation program.

To add a new partition

1. Install the software over the existing installed product.
2. Select the option for adding a new partition in the install program.
3. This will add a data source, edit the configuration files to make new entries, and add a directory structure in the folders for accommodating the new partition.
4. The installation program at the end generates a new URL for the newly added partition.



Note: Refer to *Cisco Interaction Manager Installation Guide* for details.

Editing partitions

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

To edit a partition

1. Select the partition to display its contents in the **Properties** pane.
2. Select the relevant tab to edit the properties. The tabs are listed as **General**, **Services**, **Databases**, and **Permissions**.



- a. **General:** This tab allows you to edit name, description amongst other fields. You can enable a partition from this tab as well.
 - b. **Services:** This tab allows you to select or clear the services that would work within this particular partition. Services will be explained in detail in the “Services” chapter.
 - c. **Database:** This tab lists all the databases available for this partition. Select any one database to view all its properties.
 - d. **Permissions:** From this tab you can view the permissions available to the relevant users within the System Console.
3. Not all properties are editable. The non-editable properties are grayed out.
 4. Modify the properties and save the changes.

Disabling partitions

You cannot delete a partition once it is created. However, you can disable a partition to avoid its use for a limited time period. By disabling a partition you free up the system resources.

To disable a partition

1. Select the required partition to display its properties in the **Properties** pane.
2. Select the **General** tab.
3. Click the **Enabled** field dropdown and select the **No** status.
4. This disables the partition.



Managing hosts

- ▶ [About hosts](#)
- ▶ [Editing hosts](#)
- ▶ [Deleting hosts](#)

About hosts

Hosts can be configured from the System Console for the overall system. These are the physical machines on which software processes will be running. A host can serve multiple partitions.

You can work with hosts only from the **Shared** resources node because Hosts are applicable across all partitions.

Hosts are created during the installation process. To create multiple hosts carry out the installation again.

Editing hosts

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

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

To edit a host

1. Select the required host from the **List** pane to display it in **Properties** pane.
2. From the **General** tab in **Properties** pane, modify the following fields.

Name	Value
Name *	napa
Description	Host Controller
Enabled *	Yes
Monitoring interval (ms)	60000
RMI port number *	9099

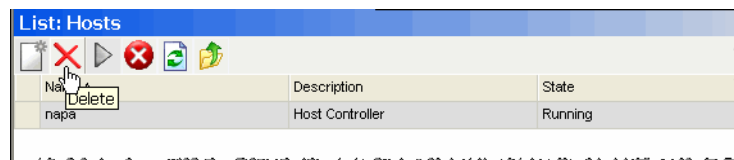
- **Enabled:** Modify the status of the Host from options given in the dropdown list.
- **Monitoring interval:** Set a monitoring interval in numerical value for the host.

Deleting hosts

You may want to delete a host if it is not required anymore. The host may also be consuming the system resources that might otherwise be useful.

To delete a host

1. Ensure that no service process or instance is running on the particular host.
2. Select the host from **List** pane.
3. Click the **Delete** button in the **List** pane to delete and confirm.





Managing services

- ▶ [About services](#)
- ▶ [About service processes](#)
- ▶ [About service instances](#)
- ▶ [Managing service processes](#)
- ▶ [Managing service instances](#)

About services

Services accomplish specialized functions within the system. For example, a dispatcher service is responsible for sending out emails from the system. Similarly other services perform varied functions for the system.

The services in System Console are of the following types:

Chat

Agent AssignmentService: This Service routes chat activities to different queues and assigns them to available agents.

Content Index

- ▶ **Article:** This service updates the index of article content in the database. When the service runs, the content index is updated every time an article is modified. It facilitates faster searches.
- ▶ **Attachment:** This service facilitates searches on different text based attachments. It filters such attachments and stores the text content in a full text-enabled database column. It then indexes the text content periodically. Any search on an attachment is carried out on this index thus enabling faster results.
- ▶ **Email:** This service updates the index of the email content in the database. This facilitates faster searches as well.
- ▶ **EmailAttachment:** Email attachment content service creates an index for newly added attachment. This index is used for searching emails attachments using some keywords. For MS SQL database this service uses Verity APIs (3rd party tool) and for Oracle database it uses Intermedia search provided by Oracle.

Email

- ▶ **Dispatcher:** 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:** 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

- ▶ **Scheduler:** This service schedules the messaging and reminder system.

Knowledge Base (KB)

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

Workflow

- ▶ **Activity Pushback:** Auto Pushback 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:** The Alarm service processes Alarm workflows 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:** This service maintains and updates the Rules Cache, KB Cache, and Queue Cache in the system. It generates a serialized file that is accessed by all rules engine instances before executing rules.
- ▶ **Workflow Engine:** This service is the main Rules engine. It uses the cache from serialized files produced by Rules Cache service, and applies rules on activities on the basis of workflows. This service handles the General, Inbound, and Outbound workflows.

Multiple processes and instances can be created of each service.

About service processes

Service Processes work across more than one customer deployment, thus minimizing the system load. This uses fewer resources on the server and maximizes the efficiency of the system. For example, one Dispatcher service process could serve one or more deployments. Service Processes have to be started in order to enable the basic functioning of the system.

About service instances

Service Instances are derivatives of Service Processes. Configure Service Instances within each customer deployment in the system, to accomplish specific functions. These instances are specific to a deployment and do not work across more than one deployments.

Managing service processes

The system offers you all the services you need for efficient functioning. To utilize these services you must create Service Processes of each service.

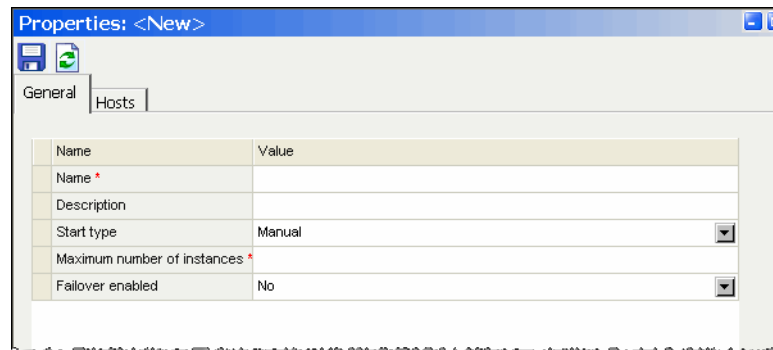
Service Processes are not running all the time. You have to start any Service Process before you can use it on your system.

Creating service processes

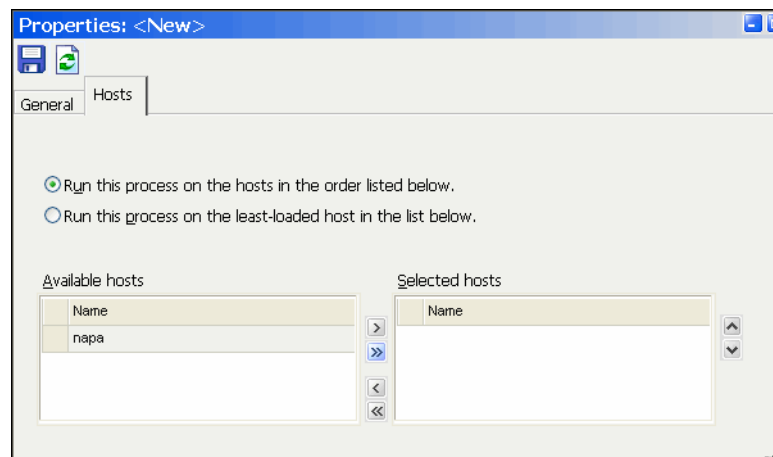
Before creating a service process, estimate your system requirements well and understand the number of customer deployments you are serving. Depending on these, you can create the number and type of service processes you require.

To create a service process

1. Select the relevant service from **Service Processes** node in the **Tree** pane.
2. Click the **New** button in **List** pane to display the attributes fields in **Properties** pane.
3. Under **General** tab, enter the following details.



- **Name and Description:** Enter the name and description to identify the process.
 - **Start type:** Select start type from the dropdown box. The service process can be started manually or set to automatic.
 - **Maximum number of instances:** Enter the maximum number of instances that this service process can have. For information on instances, see About Service Instances.
 - **Failover enabled:** Select a value from the dropdown box. If set to Yes, the process will try to restart on its own in event of any failure.
4. Under the **Hosts** tab, choose from the following two options.



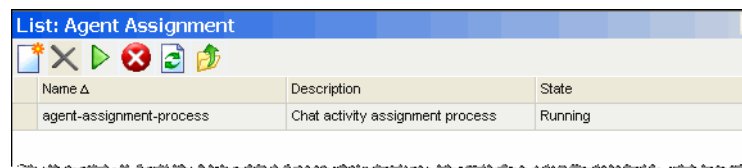
- **Run this process on the hosts in the order listed below**
 - **Run this process on the least loaded host in the list below**
5. Select the hosts from the given list.
6. Click the **Save** button to display the process in the **List** pane.

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 that you require.

To start a service process

1. Select the **Services** node in **Tree** pane.
2. Select the required service process from **List** pane.
3. Click the **Run** button in **List** pane.

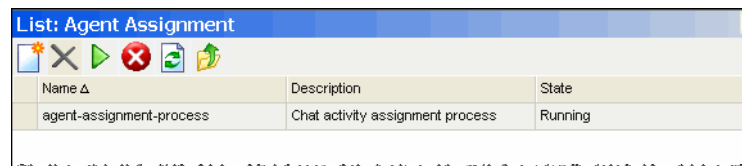


4. The process starts on the selected hosts.
5. Service processes also start when the system starts, if automatic start type is selected.

Stopping service processes

To stop a service process

1. Select the **Service Process** node in **Tree** pane.
2. Select the running service process from **List** pane.
3. Click the **Stop** button in the **List** pane.



4. The process stops working on the selected hosts.



Note: All service instances also stop, once the service process is stopped.

Managing service instances

Service instances are specific to partitions. You can manage all the activities related to instances from the individual partitions. For example if you want a particular service to run only for a specific partition, then start the Service Instance from that partition.

You can also create and delete instances as and when you deem necessary.

Creating service instances

Create service instances when you want to service a specific partition or customer deployment.

To create a service instance

1. Select the relevant service from **Service Instances** node in **Tree** pane.
2. Click new button in the **List** pane to display the attributes fields in **Properties** pane.
3. Under **General** tab, enter the following details.

Name	Value
Instance name *	agent-assignment-instance
Description	Chat activity assignment instance
Start type *	Automatic

- **Instance name:** Enter name to identify the instance.
 - **Description:** Enter a brief description.
 - **Start type:** Select start type from the dropdown list. The service process can be started manually or set to automatic.
4. Click **Save** to display the process in **List** pane.

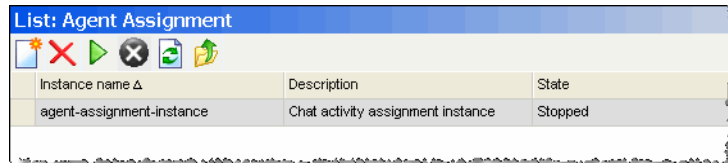


Note: The number of instances for a given Service should tally with the maximum number of Instances defined for the Service Process in Shared Resources. See "Creating Service Process."

Starting service instances

To start a service instance

1. Select the required service instance from **List** pane.
2. Click the **Run** button in the **List** pane.



3. The instance starts on the partitions.



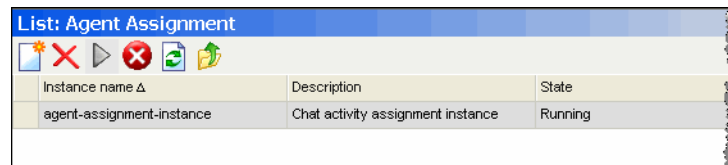
Important: More than one Service Instance cannot be started on a partition, except for Retriever, Dispatcher, and Rules.

4. Service instances also start with the system, if automatic start type is selected.

Stopping service instances

To stop a service instance

1. Select the running service instance from **List** pane.
2. Click the Stop button in the **List** pane.



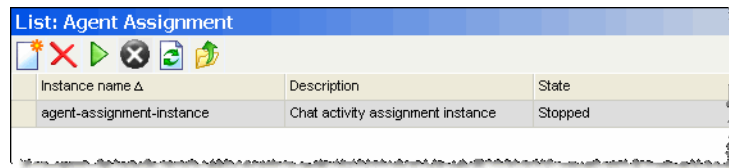
3. The instance stops running.

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. Select the required service instance from **List** pane.
2. Click the **Delete** button in **List** pane.



Instance name Δ	Description	State
agent-assignment-instance	Chat activity assignment instance	Stopped

3. Confirm the deletion.

The instance is stopped prior to being deleted.



Managing loggers

- ▶ [About loggers](#)
- ▶ [Configuring loggers](#)
- ▶ [Editing loggers](#)
- ▶ [Working with handlers for shared resources](#)
- ▶ [Using filters for shared resources](#)
- ▶ [Working with logs](#)
- ▶ [Viewing logs](#)

About 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 the client side or server side as per the settings, helping your maintenance engineers trace the cause of the problem.

The logger can log messages:

- ▶ On the console
- ▶ In a text file on the local machine
- ▶ In text and XML format on a remote machine

You can allot different levels of severity to messages. These severity levels are called trace levels. The display of messages can be filtered using these trace levels.

Messages can also be filtered based on the source of the log.

Loggers help you to keep track of the system's efficiency. You can use system logs as well as any additional logs that you might create to check for bugs, real time errors, or application performances.

Configuring loggers

Loggers cannot be created from the System Console. However, you can create log reports, which will be discussed in a subsequent section.

Ensure the following settings are taken care of, before using the logger:

1. System variable, `INSTALL_DIR` must be set to the location of the platform directory.
2. The required jar file is `egpl_logger.jar`.
3. Ensure that the entry for the `egpl_loggerconfig.properties` in the `egpl_master.properties` is correct. The `logger.configfile` property in the `egpl_master.properties` file should point to the correct location where the `egpl_loggerconfig.properties` file has been placed.

E.g. `Logger.configfile = config/egpl_loggerconfig.properties`

4. Ensure that the following directories are present.
 - `<INSTALL_DIR>/config` - The configuration file `egpl_master.properties` should be placed in this directory.
 - `<INSTALL_DIR>/logs` - The log files in which the messages get logged are created in this folder. If the 'logs' directory is not found, the Logger puts all the log files into the current working directory.

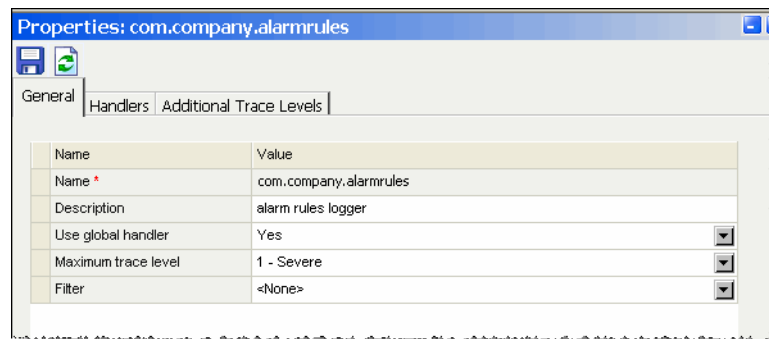
- <INSTALL_DIR>\web and <INSTALL_DIR>\lib - These help modify logger attributes from the UI.

Editing loggers

Edit a logger if you want different kind of messages to be logged than the existing ones. For example, you may want to change the trace levels to log the relevant messages.

To edit a logger

1. Select a logger to display its attributes in the **Properties** pane.
2. Edit the following fields under the **General** tab.



- **Use global handler:** select whether you want a global handler or not. Global handlers can be used in absence of any other specified handler.
 - **Maximum trace level:** Select a trace level from the dropdown list. Messages with the selected trace level as well as the ones ranked below it will be logged.
 - **Filter:** Select from the list of filters available in the dropdown list.
3. Select handlers if required from the list of **Available handlers**. Alternatively, you can also remove handlers from the **Selected handlers** list using the **Add** and **Remove** buttons in the between.
 4. Select trace levels if required from the list of **Available trace levels**. Alternatively, you can also remove them from the **Selected trace levels** list using the **Add** and **Remove** buttons in the between.

The logger name, however, is non-editable.

Working with handlers for shared resources

You can create and manage handlers only from the shared resources. Handlers help you process the data generated by loggers in a usable format.

About handlers

Handlers process the event data generated by the loggers. Handlers correspond to a physical device, such as a console or file. They usually format the data. At least one handler must be attached to a logger or the event data is lost.

The different types of handlers that can be attached to a logger are:

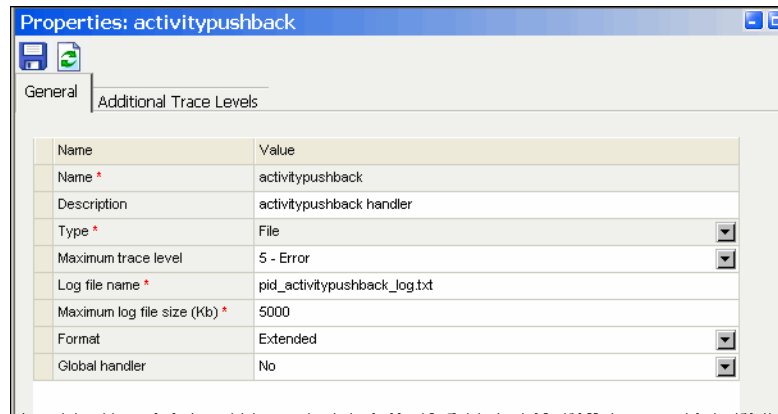
- ▶ **Console Handler:** Logs the data in a Web logic console.
- ▶ **File Handler:** Logs the data in a specified file.

Creating handlers

Apart from the global handler that is available in the system, you can create additional handlers for specific kinds of output. The handlers created from here can then be attached to a logger from the Logger node.

To create a handler

1. Select **Handlers** node from the **Tree** pane.
2. Click the **New** button from the **List** pane to display the attribute fields in the **Properties** pane.
3. In the **General** tab, enter the following key attributes amongst others.



Name	Value
Name *	activitypushback
Description	activitypushback handler
Type *	File
Maximum trace level	5 - Error
Log file name *	pid_activitypushback_log.txt
Maximum log file size (Kb) *	5000
Format	Extended
Global handler	No

- **Type** denotes the type of handler being specified. Select Console or File, for Console handler or File handler respectively.
 - **Maximum trace level** denotes the trace levels that can be logged.
 - E.g. If MaxTraceLevel is set to PERF, the messages with trace levels PERF, DBQUERY, ERROR, CONFIG, INFO, WARNING, AND SEVERE will be logged provided they have been considered for logging by the logger to which this handler is attached.
 - **Format** specifies the format of the message to be logged.
4. From the **Additional Trace Levels** tab, add the additional levels that can be logged.
 5. Click the **Save** button to display the new handler in the **List** pane.

Using filters for shared resources

Filter is another aspect of logger that can be configured from the shared resources. You may want to view logs based on specified filtering criteria. Not all messages generated by loggers would be important for your reference. In such case use a filter to sort out only the type of messages you would want to pay attention to.

About filters

Filters control the log records that are written to the output devices controlled by Handlers. Each Logger can have a filter associated with it.

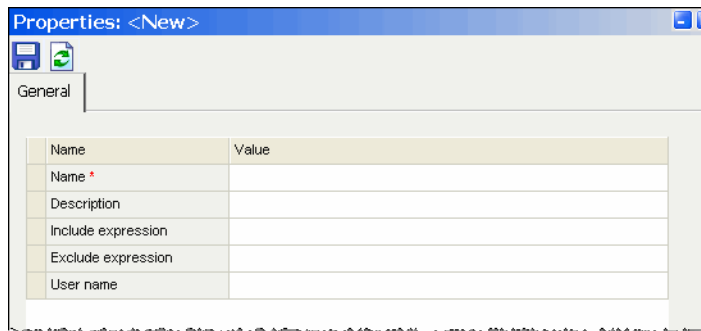
Filters help sort the criteria by which logger can display only the information that is asked for.

Creating filters

Create a filter so that you can associate it with a logger to filter its messages. The criteria include logging level, module, and time.

To create a new filter

1. Select the **Filter** node from **Tree** pane.
2. Click the New button in **List** pane to display the attribute fields in **Properties**.



3. Enter the attributes such as **Name**, and **Description**. In **Include expression**, and **Exclude expression** fields, you can enter expressions that will respectively include or exclude all logs that contain the specified expressions.
4. Click **Save** to display the new filter in the **List** pane.

Working with logs

You can create and delete log reports to suit your requirements.

Customizing log displays

The log reports can be customized to your preference. Depending on the requirements, select data and attributes that can be included or excluded from the logs.

To customize a log display

1. Select **Logs** from **Tree** pane and click new button in the **List** pane.
2. Under **General** tab, enter name and description of the log.
3. From **File** tab, select the file in which information is to be logged.
4. The **Criteria** tab allows you to select specific criteria for the log. The log display contains information bound by these specifications.
5. The **Trace Levels** tab helps you to specify trace levels, which limits the log display. In other words, logs falling within specified trace levels will only be displayed.
6. The **Report Columns** tab helps you select specific column attributes that will be displayed in the log. Thus log report will only display the required data.
7. Click the **Save** button.

Deleting log reports

To delete logs:

1. Select the **Logs** node in **Tree** pane.
2. Select the required log report in **List** pane.
3. Click delete button in **List** pane.
4. Confirm the deletion.

Viewing logs

The logs that you create, displays multiple reports on the system and application performance. You can create and view the reports logs from the **Logs** folder in the **Tree** pane.

System logs

The System logs generate reports for the entire system across all partitions and applications.

To view a log:

1. Select the **Logs** folder in **Tree** pane.
2. Select the required log report in **List** pane.
3. Click start button in **List** pane.
4. The report result is displayed in a new window. The attributes that are selected during creation of the log (see, Customizing Log Displays) determine log report.

Application logs

The application logs will generate reports for specific partition or application.

To view a log:

1. Select the **Logs** folder in **Tree** pane.
2. Select the required log report in **List** pane.
3. Click start button in the **List** pane.
4. The report result is displayed in a new window. The attributes that are selected during creation of log (see, Customizing Log Displays) determine the log report.



Monitoring the system

- ▶ [About monitors](#)
- ▶ [Configuring monitors](#)
- ▶ [Monitoring hosts](#)
- ▶ [Monitoring services](#)
- ▶ [Deleting monitors](#)

About monitors

Monitors enable you as an administrator to keep account of the status of system resources. You can monitor various actions from the System Console at shared resource level as well as partition level.

Configuring monitors

Create different monitors from Monitors node to enable periodic checks on the system resources. These monitors help you keep an account of which system resource is running. This helps you decide whether you want to stop a particular resource that is not in use.

Configure monitors such that only the required attributes are displayed in results. You can also save monitors for repeated use.

To configure a monitor

1. Select the **Monitors** node in **Tree** pane.
2. Click the **New** button in the **List** pane to display the fields in **Properties** pane.
3. Under **General** tab, enter the following details.

Name	Value
Name *	New monitor
Description	
Start type *	Manual

- a. **Name:** Name represents the type of monitor to be created
 - b. **Description:** A brief description helps in understanding the function.
 - c. **Start type:** The monitor can be enabled to run manually or automatically.
4. Under **Objects** tab, select the object to be monitored. It could be a host, service process, or service instance.
 5. From the **Attributes** tab, select attributes of the selected object to be monitored. The attributes selected here will be displayed in monitoring reports, when run.

6. Select a notification type from **Notification** tab. The **Conditions** sub-tab allows you to create specific conditions for enabling notifications. For example, for a local host if the host id is 020, a notification can be sent in prescribed format. Notifications can be displayed according to preference such as alerts, dialog windows, and mails.

Monitoring hosts

Hosts are monitored from the moment you start running the host. You can also create host monitors from the **Monitors** section

Starting host monitors

Create monitors to keep a watch on the enabled hosts. Such monitors run configured rules and show you the captured data.

To run a monitor

1. Select the **Monitors** node in **Tree** pane.
2. Select the required monitor name from **List** pane.
3. Click Run button in **List** pane.
4. The host monitor is displayed according to the attributes that have been defined.
5. Hosts can be monitored over the following features.
 - Free bytes
 - Host ID
 - Host Name
 - Last Ping Time
 - Start Time
 - Stop Time
 - State
 - Status description

Stopping host monitors

The monitoring of entries of a host is stopped when you stop the host from running.

To stop a host monitor

1. Select the host from the **List** pane.
2. Click the **Stop** button.

Monitoring services

You can monitor service processes and instances by creating monitors for each of them. These monitors help you keep a track of the service performance and help you decide any change in requirement. Almost all the important attributes can be monitored depending on the ones you chose to display.

Monitoring service processes

Create monitors to keep a watch on the service processes. These monitors display data according to the selected attributes such as the process name, id, start time, and so on.

To run a monitor

1. Select the **Monitors** node in **Tree** pane.
2. Select required monitor name from the **List** pane.
3. Click Run button in the **List** pane.
4. The monitor displays the attributes that you have defined.
5. Depending upon the notification you have selected while creating, the monitor is displayed in a new window or toolbar alert. You may also receive an email if you have configured the monitor accordingly.

Processes are also monitored from the moment the administrator starts the service process. Such data is recorded in the database.

Monitoring service instances

You can also create monitors to keep a watch on service instances. These monitors display data according to the selected attributes such as the process name, id, start time, and so on.

To run a monitor

1. Select the required monitor name from **List** pane.
2. Click Run button in **List** pane.

3. The monitor displays the attributes that you have defined.
4. Depending upon the notification you have selected while creating, the monitor is displayed in a new window or toolbar alert. You may also receive an email if you have configured the monitor accordingly.

Instances are also monitored from the moment the administrator starts the service process. Such data is recorded in the database.

Deleting monitors

To delete monitors

1. Select the **Monitors** node in **Tree** pane.
2. Select required monitor in the **List** pane.
3. Click delete button in the **List** pane.
4. Confirm the deletion.