



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

For Unified Contact Center Express

Release 4.2(1)
July 2007

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

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

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

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

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

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

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0705R)

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

Cisco Unified Web and E-Mail Interaction Manager System Console User's Guide: For Unified Contact Center Express
© 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	13

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: Partitions	19
About partitions	20
Adding partitions	20
Managing partitions	21
Disabling partitions.	21
Managing service instances	22
Increasing the number of service instances.	22
Removing service instances	23
Viewing database details	23
Assigning permissions	25
Chapter 4: Managing hosts	27
About hosts	28
Editing hosts	28
Deleting hosts	29
Stopping hosts.	29
Starting hosts	29
Chapter 5: Services	31
About services, service processes, and service instances.	32
Services	32
Service processes	34
Service instances.	34
Managing service processes	34
Creating service processes	34
Deleting service processes	35
Increasing the number of instances for service processes	36
Starting service processes	36
Stopping service processes	37
Managing service instances	37
Creating service instances.	37
Deleting service instances.	38

Starting service instances	39
Stopping service instances	39
Adding aliases to retriever instances	40

Chapter 6: Loggers 42

About loggers, handlers, and filters	43
Loggers	43
Handlers	43
Filters	43
Managing handlers	44
Creating handlers	44
Deleting handlers	45
Managing filters	45
Creating filters	46
Deleting filters	47
Editing loggers	47

Chapter 7: Monitors 49

About monitors	50
Host monitors	50
Service process monitors	51
Service instance monitors	51
Configuring monitors	52
Deleting monitors	55
Starting monitors	55

Preface

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

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

About this guide

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

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

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	A file name or command. Or, text that must be typed by the user.
<i>Variable</i>	User-specific text, provided by the user.


Document conventions

Other learning resources

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

Online help

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

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

Online help options

Document set

The Cisco Unified Web and E-Mail Interaction Manager documentation is available in the **Documents** folder on the product CD. It includes the following documents:

- ▶ *Cisco Unified Web and E-mail Interaction Manager Release Notes*
- ▶ *Cisco Unified Web and E-mail Interaction Manager System Requirements*
- ▶ *Cisco Unified Web and E-mail Interaction Manager Solutions Reference Network Design Guide*
- ▶ *Cisco Unified Web and E-mail Interaction Manager Browser Settings Guide*
- ▶ *Cisco Unified Web and E-mail Interaction Manager Administration Console User's Guide*
- ▶ *Cisco Unified Web and E-mail Interaction Manager Agent Console User's Guide*
- ▶ *Cisco Unified Web and E-mail Interaction Manager Knowledge Base Console User's Guide*
- ▶ *Cisco Unified Web and E-mail Interaction Manager Reports Console User's Guide*
- ▶ *Cisco Unified Web and E-mail Interaction Manager Supervision Console User's Guide*
- ▶ *Cisco Unified Web and E-mail Interaction Manager System Console User's Guide*
- ▶ *Cisco Unified Web and E-mail Interaction Manager Tools Console User's Guide*

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

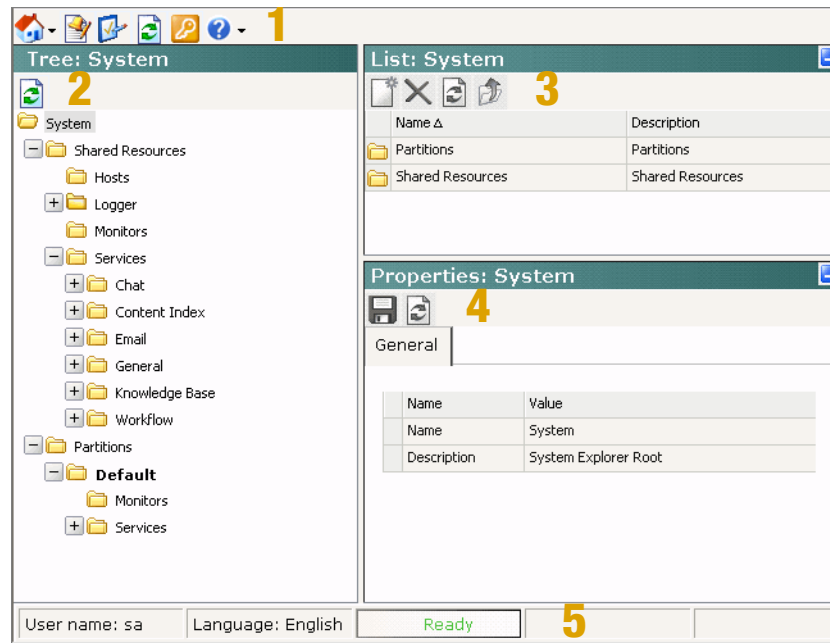
Loggers are used for maintaining and debugging applications. Developers embed various types of trace messages in the code at critical points. These trace messages are logged in appropriate files on client side or server side as per the settings, helping the maintenance engineers trace the cause of a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



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).

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 Unified Web and E-mail 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 Unified Web and E-mail Interaction Manager Installation Guide*.

3 Partitions

- ▶ [About partitions](#)
- ▶ [Adding partitions](#)
- ▶ [Managing 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

- ▶ Refer to *Cisco Unified Web and E-mail Interaction Manager Installation Guide* for details.

Managing partitions

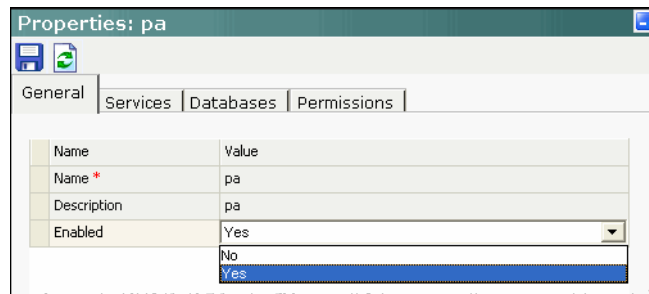
You may need to edit a partition if you want to adapt it to a changing business unit. You can modify the properties of different partitions according to changing requirements.

Disabling partitions

You cannot delete a partition once it is created. However, you can disable a partition to avoid its use. By disabling a partition you free up the system resources. Once you disable a partition no user in that partition can log in to the application. If there are any users who are all ready logged in to the application, they are shown a message that the partition has been disabled, and they are logged out of the application. Before disabling the partition stop all the instances running in the partition.

To disable a partition

1. In the Tree pane, browse to **System > Partitions**.
2. In the list pane, select the partition you want to disable.
3. In the Properties pane, go to the General tab and in the **Enabled** field select **No**.



Disable a partition

4. Click the **Save**  button.

Managing service instances

Increasing the number of service instances

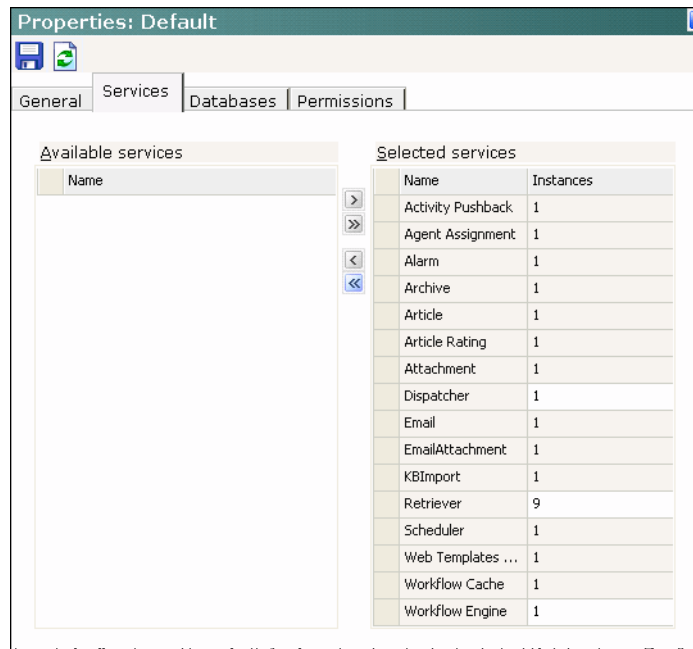
For each partition you can increase the number of service instances for three services. They are:

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

For rest of the services each partition can have only one instance.

To increase the number of instances

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 a partition

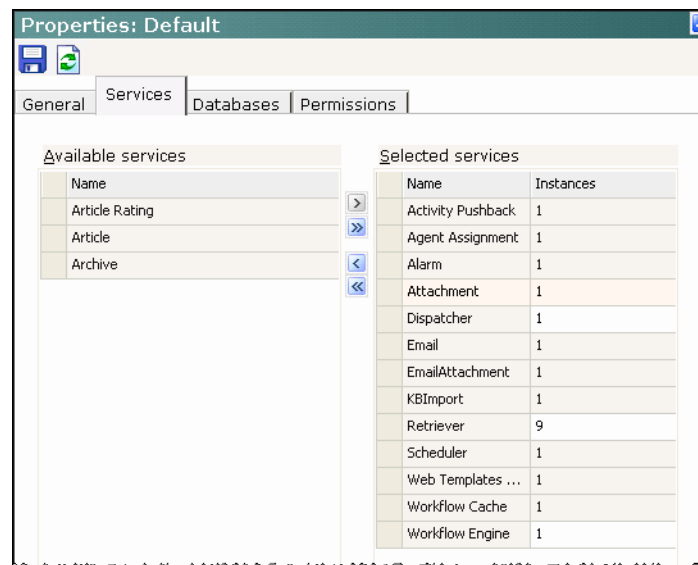
4. Click the **Save**  button.

Removing service instances

If your partition doesn't need any service, remove its service instance from the partition. This way no one in the partition can start the service instance for that partition and it frees up the resources. Make sure you stop the service process before removing it from the partition. If needed, you can add it back at any point.

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 instance you don't want to use.



Remove service instances not needed for the partition

4. Click the **Save**  button.

Viewing database details

You can't edit this information from the System Console.

To view the database details

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 Databases tab. It shows the details about the following databases.
 - **Customer DB**
 - **Master DB**
 - **Mail DB**
 - **Archive DB**
 - **Archive app DB**
 - **Knowledge DB**
 - **Campaign DB**
 - **IPCC 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**

Database Name	Property Name	Value
customer_db	Name	
master_db	Name	Platform_MSSQL_Pool
mail_db	Active	y
archive_db	Type	basic
archive_app_db	CapacityIncrement	2
knowledge_db	InitialCapacity	1
campaign_db	MaxCapacity	50
ipcc_db	DriverName	com.microsoft.jdbc.sqlserver.SQL...
	User	eGActiveDB_IPCC
	Password	*****
	Url	jdbc:microsoft:sqlserver://sbahl04...
	Targets	
	Vendor	mssql
	DriverVendor	

View database details of a partition

Assigning permissions

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

- Own
- View
- Edit
- Administer

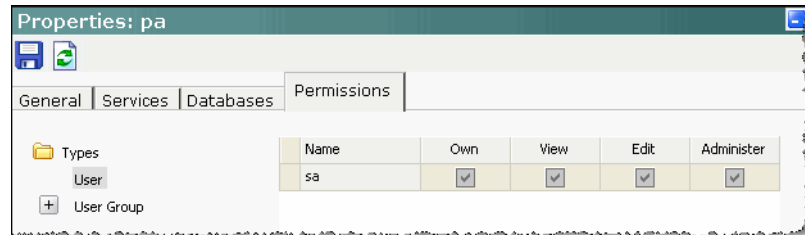


Important: Permissions can be given only to users and user groups who have appropriate actions assigned to them. When permissions are given to a user group, all users in that user group get those permissions automatically.

To assign permissions

1. In the Tree pane, browse to **System > Partitions**.
2. In the List pane, select a partition.

3. In the Properties pane, go to the Permissions tab and assign permissions to the users and user groups on the partition.



Assign permissions to users and user groups

4. Click the **Save**  button.



Managing hosts

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

About hosts

Hosts can be configured from the System Console for the overall system. These are the physical machines on which software processes will be running. 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. As of now a deployment can have only one host.

Editing hosts

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

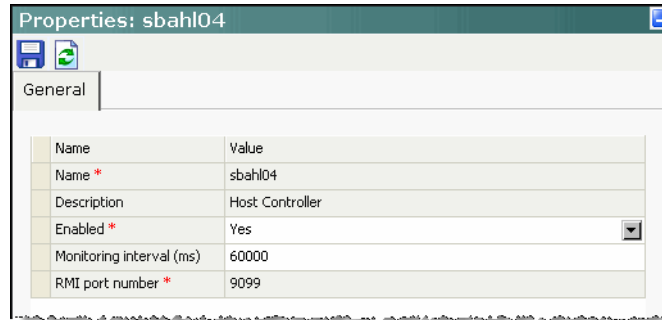
You may want to edit a host property to change its availability in the system. You may also want to monitor the host functions frequently and hence want to change its monitoring interval.

To edit a host

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

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

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

To start a host

1. In the Tree pane, browse to **System > Shared Resources > Hosts**.

2. In the List pane, select the host.
3. In the List pane toolbar, click the **Start**  button.

5 Services

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

About services, service processes, and service instances

Services

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

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 of each service. Services are of following types.

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

Chat service

- ▶ **Agent Assignment service:** This Service routes chat activities to different queues and assigns them to available agents.

Content Index service

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

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

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

Knowledge Base (KB) services

- ▶ **Article Rating service:** 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 service:** This service imports folders and articles from external file system to the knowledge base. The service imports folders and articles only from the external content folders specified in the knowledge base. The files are imported as knowledge base articles (either as internal or external attachments) and directories as folders. If any file is updated on the external file system, since the last run of service, the service also updates those files in knowledge base.

Workflow services

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

Service processes

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.

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

For each service, a service process is provided in the system. In addition to these you can create new service processes.


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

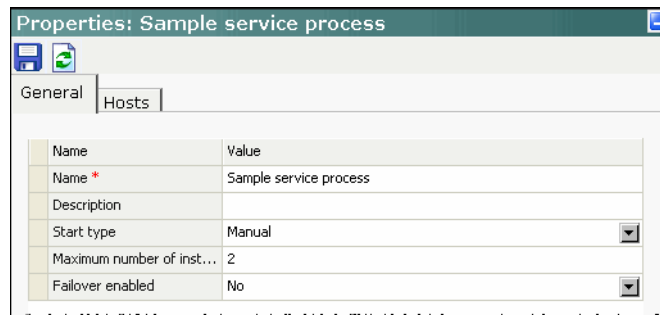
Creating service processes

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. 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**
 - **Automatic**
 - **On demand**
 - **Maximum number of instances:** Type the maximum number of instances this service process can have.
 - **Failover enabled:** This feature is not available in this release. From the dropdown list select No.



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

Delete the service processes that are no more required in the system. Before you delete the service process make sure it is not running.

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

When the deployment has more than one partition and you need to run the service instances for all those partitions, then there is a need to increase the number of instances that can be associated with each process.

Also, for three services there can be more than one service instance in each partition. You can increase the number of instances for these services for a partition. The three services are:

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


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 in each partition.

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 the system resources. Sometimes you need to stop and start a service process after making some changes in its properties. For example, when you increase or decrease the number of service instances that can be associated with a service process, you need to stop and start the 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 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

By default a service instance is provided for each service in the system. In addition to these you can create new service instances for the services. In a partition only three services can have more than one instance running at a time. These three services are:

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

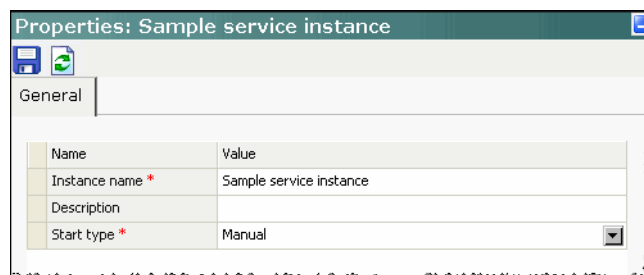
To create a service instance

1. In the Tree pane, browse to **System > Partition > *Your Partition* > 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**
 - **Automatic**



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

Set the general properties

5. For retriever service instances, there is an additional Input tab. On the Input tab, select the aliases from the available list of aliases.
6. 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, “Increasing the number of instances for service processes” on page 36.

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 > *Your Partition* > 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 each 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 36.
- ▶ Increase the number of instances that can be running in the particular partition. For details, see “Increasing the number of service instances” on page 22.

To start a service instance

1. In the Tree pane, browse to **System > Partition > *Your Partition* > 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 partition, except for Retriever, Dispatcher, and Rules.

Stopping service instances

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

To stop a service instance


1. In the Tree pane, browse to **System > Partition > *Your Partition* > 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 > *Your Partition* > 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.
6. Also, stop and start all the dispatcher instances for the partition.

6 Loggers

- ▶ [About loggers, handlers, and filters](#)
- ▶ [Managing handlers](#)
- ▶ [Managing filters](#)
- ▶ [Editing loggers](#)

About loggers, handlers, and filters

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.

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.

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.

Managing handlers

Creating handlers

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

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

To create a handler

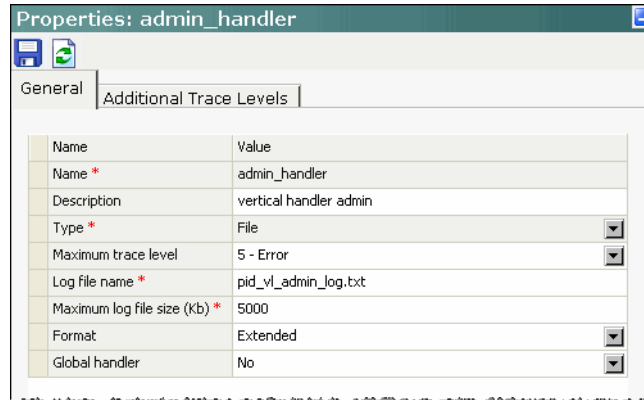
1. In the Tree pane, browse to **System > Shared Resources > Logger > Handlers**.
2. In the List pane toolbar, click the **New**  button.

The Properties pane refreshes to show the properties handler.


3. In the Properties pane, on the General tab provide the following details.
 - **Type:** First select the type of handler you want to create. The options available are:
 - **File**
 - **Single File**
 - **Console**

Once you select the type, the other properties on the General tab are enabled.

- **Name:** Provide a name for the handler.
- **Description:** Provide a brief description.
- **Maximum trace level:** Select the maximum trace levels that can be logged. For example, If Maximum trace level is set to perf, the messages with trace levels perf, dbquery, error, config, info, warning, and severe are logged, provided they have been considered for logging by the logger to which this handler is attached.
- **Log file name:** Specify the name of the log file. This option is not available for console handlers.
- **Maximum log file size (KB):** Specify the maximum size of the log file. This option is not available for console handlers.
- **Format:** Specify the format of the message to be logged. Select from standard or extended format.
- **Global handler:** Select Yes if you want to make this the global handler. There can be one global handler in the system, and by default **consolehandler** is the global handler.




Set the general properties

4. Next, on the Additional Trace Levels tab select the additional levels to be logged.
5. Click the **Save**  button.

Deleting handlers

You cannot delete a handler if it is the global handler or if it is associated with a logger.

To delete a handler

1. In the Tree pane, browse to **System > Shared Resources > Logger > Handlers**.
2. In the List pane, select the handler you want to delete.
3. In the List pane toolbar, click the **Delete**  button.


Managing filters

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 record.

Creating filters

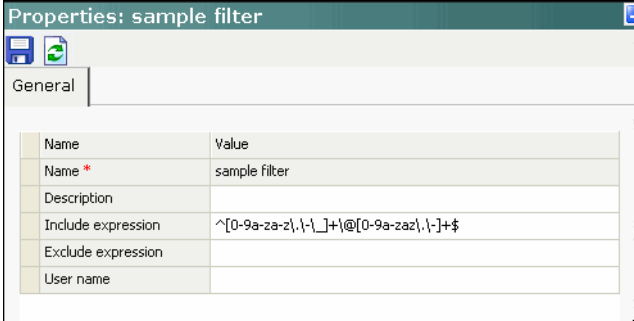
Create a filter so that you can associate it with a logger to filter its messages.

To create a filter

1. In the Tree pane, browse to **System > Shared Resources > Logger > Filters**.
2. In the List pane toolbar, click the **New**  button.

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

2. In the Properties pane, on the General tab provide the following details.
 - **Name:** Provide a name for the filter.
 - **Description:** Provide a brief description.
 - **Include expression:** Type the regular expressions based on which you want to filter the logs. The logs with the expression provided in this field will be included.
 - **Exclude expression:** Type the regular expressions based on which you want to filter the logs. The logs with the expression provided in this field won't be included. Example of a regular expression: `^[0-9a-zA-Z\.\-_]+\@[0-9a-zA-Z\.\-]+\$,` this expression refers to a format X@Y. Z (john@cisco.com).
 - **User name:** Type the user name of the user for which you want to see the logs. When you use this filter it only shows the logs related to the actions done by this particular user in the system.



Name	Value
Name *	sample filter
Description	
Include expression	^[0-9a-zA-Z\.\-_]+\@[0-9a-zA-Z\.\-]+\\$
Exclude expression	
User name	


Set the general properties

3. Click the **Save**  button.

Deleting filters

You cannot delete a filter if it is associated with a logger.

To delete a filter

1. In the Tree pane, browse to **System > Shared Resources > Logger > Filters**.
2. In the List pane, select the filter you want to delete.
3. In the List pane toolbar, click the **Delete**  button.

Editing loggers

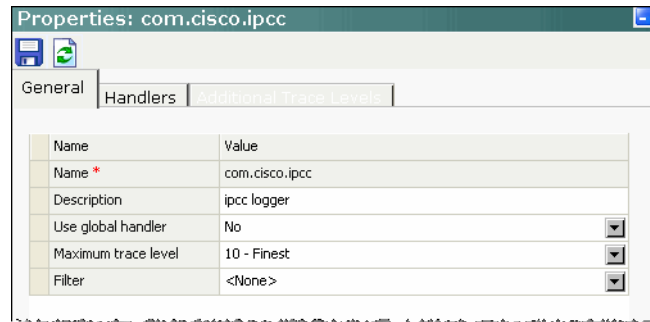
Edit a logger if you want different kind of messages to be logged than the existing ones. For example, you may want to change the trace levels to log the relevant messages. You cannot create new loggers or delete the existing ones from the System Console.

To edit a logger


1. In the Tree pane, browse to **System > Shared Resources > Logger > Loggers**.
2. In the List pane, select the logger you want to edit.

The Properties pane refreshes to show the properties of the selected logger.

3. In the Properties pane, on the General tab view the properties of the selected logger. Except for the name of the logger you can edit all the other properties of the loggers.
 - **Name:** Displays the name of the logger. You can't change the name of the logger.
 - **Description:** Displays the description of the logger.
 - **Use global handler:** Select whether the logger should use the global handler 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.



Edit the general properties

4. Next, on the Handlers tab, select the handlers from the available handlers list.
5. Next, on the Additional Trace Levels tab, select the additional trace levels for the logger.
6. 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 partition level you can monitor service instances. For each monitor you specify the objects you want to monitor, i.e. the hosts, service processes, or service instances, and the attributes of the objects to be monitor. For each object, different attributes are available for monitoring. For example, you can monitor the free bytes, start time, stop time, and state of hosts.

Host monitors

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

Objects available for monitoring

- ▶ *Host_name* - DSM Controller
- ▶ *Host_name* - Host Controller
- ▶ *Host_name* - License Manager Server
- ▶ *Host_name* - Remote Session Manager Server
- ▶ *Host_name* - RMI Registry Server
- ▶ *Host_name* - RMID Registry Server
- ▶ *Host_name* - Application Server
- ▶ *Host_name* - JMS Server
- ▶ *Host_name* - Web Server
- ▶ *Database_server_name* - Database server

Attributes available for monitoring

- ▶ **Host ID:** ID of the host being monitored.
- ▶ **Host Name:** Name of the host being monitored.
- ▶ **Free bytes:** Disc space available on the host.
- ▶ **State:** State of the host. The state can be waiting, running, or stopped.
- ▶ **Status description:** Description of the state of the server.

- ▶ **Start Time:** Time when the host was started.
- ▶ **Stop Time:** Time when the host was stopped.
- ▶ **Last Ping Time:** Last time the DSM pinged the host.

Service process monitors

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

Attributes available for monitoring

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

Service instance monitors

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

Attributes available for monitoring

- ▶ **Host ID:** ID of the host on which the service process is running.
- ▶ **Host Name:** Name of the host on which the service process is running.
- ▶ **Instance ID:** ID of the service instance being monitored.
- ▶ **Instance Name:** Name of the service instance being monitored.

- **Process ID:** ID of the service process with which the instance is associated.
- **Process Name:** Name of the service process with which the instance is associated.
- **State:** State of the instance. The state can be waiting, running, or stopped.
- **Last Run Time:** Time when the instance was last run.
- **Start Time:** Time when the service instance was started.
- **Stop Time:** Time when the service instance was stopped.
- **Processed in last run:** Number of activities processed when the instance last ran.
- **Processing Time (ms):** Time taken to process the activities.
- **Pending:** Number of pending email.
- **Emails Skipped:** Number of skipped emails.
- **Throughput:** Total number of activities processed since the instance was started.
- **Unable to Send:** Number of emails unable to send.

Attributes available for monitoring for aliases

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

Configuring monitors


Create different monitors to enable periodic checks on the system resources and 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

don't want to run the monitors automatically, run them manually whenever you need them.

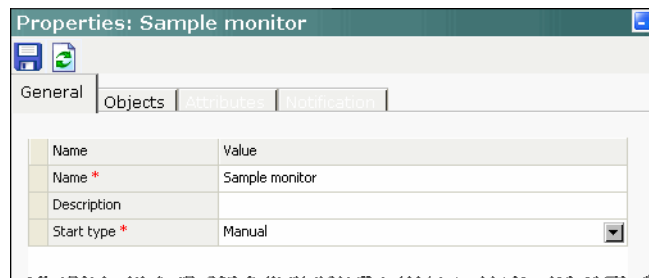
To configure a monitor

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 > *Your Partition* > Monitors.**


2. In the List pane toolbar, click the **New**  button.

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

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

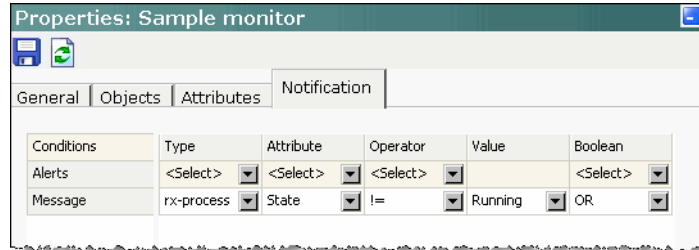


Set the general properties

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

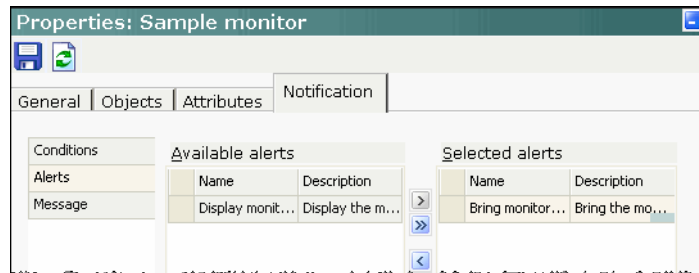
7. On the Notification tab, in the Conditions section, specify the condition when a notification should be sent.



Configure conditions for notification

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

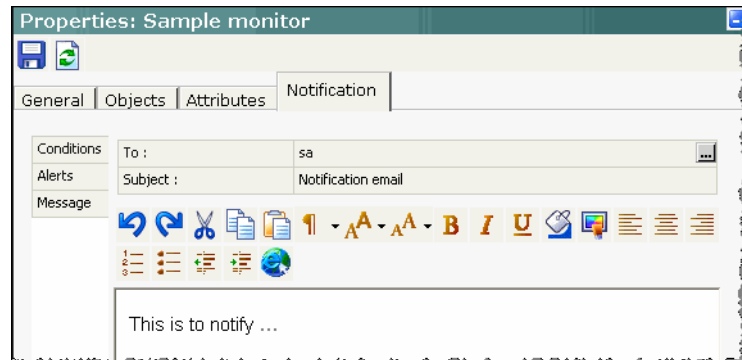
8. Next, in the Alerts section, you can set the alert type as:
 - **Display monitor window**
 - **Bring monitor window to the front**



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.

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 don't 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 > *Your Partition* > 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 don't 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 > *Your Partition* > Monitors**.
2. In the List pane, select the monitor you want to start.
 3. In the List pane toolbar, click the **Start**  button.