

Orbix Management User Guide

V6.3.14

Table of Contents

Preface	7
Audience	7
Related documentation	7
Assumptions	7
Document conventions	8
Introduction to Orbix Management	9
Orbix Management Tools	9
Administrator Web Console	12
Orbix Management Service	14
Orbix Configuration Explorer	15
Orbix Configuration Authority	17
Orbix Management Tasks	18
Getting Started with the Web Console	21
Before Starting the Web Console	21
Starting the Web Console	23
Navigating the Web Console	27
Administrator Web Console Icons	30
Managing Applications in the Web Console	33
Monitoring Managed Applications	33
Controlling Managed Servers	36
Managing the ORB Core	40
Managing Events in the Web Console	45
Starting the Events Console	45
Viewing Events	46
Management Service Configuration	49
Management service scope	49
Example configuration file	49
Orbix Configuration Explorer example	50
Configuring the Event Log	50

Configuring the event log filter	51
Sending the log output to a file	51
Configuring the local log stream	51
Configuring Resource Agents	52
Resource agents	52
Configuring a resource agent file	52
Configuring resource agent timeouts	53
Configuring Event Listeners	53
Configuring an event listener file	53
Configuring an event listener timeout	54
Configuring Event History	54
Event history	54
Configuring an event history file	54
Configuring event history memory	55
Configuring event history purges	55
Configuring Event Filters	55
Configuring an event severity file	55
Configuring an event filter threshold file	56
Configuring a default event severity file	56
Configuring Event Processing	57
Consolidated logging	57
Enabling consolidated logging	57
Configuring an idle event period	58
Configuring the logfile filter	58
Configuring the Management Service Web Server	58
Configuring the web server	58
Orbix Configuration Explorer example	59
Finding Configuration Information	60
Orbix Configuration Authority	60
Starting the Orbix Configuration Authority	61

Viewing Configuration Information	63
Managing Configuration Settings	66
Orbix Configuration Explorer	66
Viewing Configuration Settings	69
Finding Configuration Settings	73
Modifying Configuration Settings	75
Creating Configuration Settings	78
Deleting Configuration Settings	82
Management Service Configuration	84
Management service scope	84
Example configuration file	84
Orbix Configuration Explorer example	85
Configuring the Event Log	85
Configuring the event log filter	86
Sending the log output to a file	86
Configuring the local log stream	86
Configuring Resource Agents	87
Resource agents	87
Configuring a resource agent file	87
Configuring resource agent timeouts	88
Configuring Event Listeners	88
Configuring an event listener file	88
Configuring an event listener timeout	89
Configuring Event History	89
Event history	89
Configuring an event history file	89
Configuring event history memory	90
Configuring event history purges	90
Configuring Event Filters	90
Configuring an event severity file	90
Configuring an event filter threshold file	91

Configuring a default event severity file	91
Configuring Event Processing	92
Consolidated logging	92
Enabling consolidated logging	92
Configuring an idle event period	93
Configuring the logfile filter	93
Configuring the Management Service Web Server	93
Configuring the web server	93
Orbix Configuration Explorer example	94
Enterprise Performance Logging	95
Introduction	95
Configuring Performance Logging	96
Logging Message Formats	103
SNMP integration	107
SNMP gateway	107
SNMP gateway plugin	108
Configuring the SNMP Gateway	108
Configuring the SNMP gateway plugin	108
Specifying SNMP managers	109
SNMP manager list format	109
Specifying SNMP management events	110
Example SNMP management events	110
Specifying SNMP event severities	110
Specifying severities using the command line	111
Installing the Orbix MIB file	112
Glossary	113
Notices	116
Copyright	116
Trademarks	116
Examples	116
License agreement	116

Corporate information	117
Contacting Technical Support	117
Country and Toll-free telephone number	117

Preface

This guide explains how to use the Orbix management tools, and how to configure the Orbix management service. Orbix management tools enable you to manage component-based distributed enterprise applications. Orbix management tools are integrated with Orbix's Adaptive Runtime Technology (ART). This enables them to provide seamless management for the Orbix product range. They can be used across different platform and programming language environments.

Audience

This guide is aimed at administrators managing distributed enterprise environments, and developers writing distributed enterprise applications. Administrators do not require detailed knowledge of the technology that is used to create distributed enterprise applications.

Related documentation

The Orbix library includes the following related guides:

- Orbix Management Programmer's Guide
- Orbix Administrator's Guide

Assumptions

This guide assumes that the reader is familiar with the key concepts of Administrator as described in the Introduction, before proceeding to the other parts. Parts II and III are fully self-contained, and neither assumes familiarity with the other.

Document conventions

This guide uses the following typographical conventions:

Constant width	Constant width font represents commands and literal names of items (such as classes, functions, and variables). For example, constant width text might be used for the <code>java it.server</code> command.
Italic	Italic words in normal text represent emphasis and new terms (for example, <i>Administrator Web Console</i>).
Code italic	Italic words or characters in code and commands represent variable values that you must supply; for example:
Bold	Bold font is used to represent menu item selections, for example:
	To start a selected server, chose Control>Start from the menu bar.

This guide may use the following keying conventions:

	Horizontal or vertical ellipses in format and syntax descriptions indicate that material has been eliminated to simplify a discussion.
[]	Brackets enclose optional items in format and syntax descriptions.
{}	Braces enclose a list from which you must choose an item in format and syntax descriptions.
	A vertical bar separates items in a list of choices enclosed in { } (braces) in format and syntax descriptions.

Introduction to Orbix Management

The Orbix management tools enable you to manage component-based distributed enterprise applications. This section introduces these tools and outlines typical administration tasks.

Orbix Management Tools

The Orbix management tools enable you to manage and configure component-based distributed enterprise applications. They are integrated with Rocket Software's *Adaptive Runtime Technology* (ART). This enables them to provide seamless management of Orbix and any applications developed using it.

Orbix management tools are not aimed solely at any specific technology (for example, CORBA, J2EE, or Web services), but provides a generic management paradigm that enables the application to be managed without the administrator requiring knowledge of the technology used to create that application.

Orbix management scope

Orbix management tools enable you to manage and configure Orbix products, and distributed applications that have been developed using these products.

Assumptions

Orbix management tools do not assume that you are familiar with any of these products. What is required is a basic understanding of distributed applications, regardless of whether they are based on CORBA, J2EE, or Web services. You can use Orbix management tools to manage any Java or C++ system that has been enabled for management.

Components

Orbix management tools include the following main components:

- Administrator Web Console
- Orbix Management Service
- Orbix Configuration Explorer
- Orbix Configuration Authority

This guide explains how to use these tools.

Note

The Administrator Web Console, Orbix Management Service and Orbix Configuration Explorer are no longer automatically installed. They are available as an optional component. To install, please download and extract the GUI components archive and follow the installation instructions.

The GUI components archive can be downloaded from our Software License & Download (SLD) site.

The GUI components have been separated from the product as they do not fully comply with the Section 508 and WCAG accessibility requirements and guidelines. It is intended that future product releases will include updated GUI components that comply with the relevant accessibility guidelines.

Administrator Web Console

The *Administrator Web Console* provides a web browser interface to the Orbix management tools. It enables you to manage applications and application events from anywhere, without the need for download or installation. It communicates with the management service using HTTP (Hypertext Transfer Protocol), as illustrated in Figure 1.

Orbix Management Service

The *Orbix management service* is the central point of contact for accessing management information in a *domain*. A domain is an abstract group of managed server processes within a physical location. The management service is accessed by both the Administrator Web Console and by the Orbix Configuration Explorer.

Note

Managed applications can be written in C++ or Java. The same management service process (iona_services.management) can be used by EJB and CORBA (Java and C++) applications.

Orbix Configuration Explorer

The Orbix Configuration Explorer is a Java graphical user interface (GUI) that enables you to manage your configuration settings. It communicates with your Configuration Repository (CFR) or configuration file using IIOP (Internet Inter-ORB Protocol).

Orbix Configuration Authority

The Orbix Configuration Authority provides a web browser interface to descriptive information about all Orbix configuration settings. You can browse and search for information about Orbix configuration variables in your CFR or configuration file.

Figure 1 Management Overview



Additional features

Application programmers can add instructions to their code to monitor specific components in their system. This is known as adding management *instrumentation*.

In addition, Orbix also provides support for integration with *Enterprise Management Systems*.

Adding management instrumentation

Orbix products provide default instrumentation that publishes core information to the management service for any application built using these products.

However, programmers might also wish to add custom instrumentation to an application to suit their needs. Orbix therefore enables full instrumentation of server code. For information on how to write instrumentation code, see the *Orbix Management Programmer's Guide*.

Integrating with Enterprise Management Systems

Performance logging plugins enable Orbix to integrate effectively with Enterprise Management Systems (EMS), such as IBM Tivoli™, HP OpenView™, CA Unicenter™, or BMC Patrol™.

These systems enable system administrators and production operators to monitor enterprise-critical applications from a single management console. This enables them to quickly recognize the root cause of problems that may occur, and take remedial action. For details of how to configure performance logging, see Enterprise Performance Logging.

Administrator Web Console

The Administrator Web Console provides a standard web browser interface to explore and manage distributed applications. The Administrator Web Console uses HTML and JavaScript to create a standard explorer view to represent the data.

Figure 2 shows an example Administrator Web Console interface.

Figure 2 Administrator Web Console

🚰 IONA Administrator - Microsoft Interne	t Explorer			
File Edit View Favorites Tools Help				
🖙 Back 🔹 🔿 🚽 🔕 😰 🚮 🛛 🐼 Search	📓 Favorites 🛛 🛞 Me	dia 🧭 🛃 🎒 🖬 🗒		
Address 🎼 https://summer:53186/admin/index	Address 🖉 https://summer:53186/admin/index.do 🗾 Links 🌺			
╊ 🖻 🖋 😮 Ĥ				
 	🍈 secur	anaged Object e-Sample-domain nple-domain:type=Domain,name=secure-sample-domain		
E iona_services.naming.summer	Attribute	Value		
	<u>Name</u>	secure-sample-domain		
	<u>Servers</u>	{ iona_services.otstm.summer, Management Server, iona_services.locator.summer, iona_services.node_daemon.summer, iona_services.naming.summer }		
A M				
🙆 Servers		📄 🔒 🧱 Local intranet 🏾 🎢		

Multiple applications and domains

You can use one instance of the Administrator Web Console to manage multiple applications in a single domain. You also can use multiple instances of the web console to manage multiple domains from a single machine. This is shown in Figure 3.

Interaction with the management service

Each Orbix management service makes management data available using a special URL. The management service is the central point of contact for management information in each domain. It publishes information about all managed servers within its domain.

Management architecture

Figure 3 gives an overview of the management architecture. Each Administrator Web Console interacts with one management service only. This means that each console can administer the managed servers in one of the two domains only.

Multiple instances of the web console can interact with the same management service through the same HTTP port.

Figure 3 Administrator Architecture



Orbix Management Service

The Orbix management service is the central point of contact for accessing management information in a domain. The management service acts as a buffer between managed applications and management tools.

Management information

The management service maintains key state information, reducing the need to constantly access the managed applications, and thereby improving performance.

The management service stores and publishes information about all managed servers within its domain. It exposes attributes, operations, and events for all managed servers in a domain. The management service also stores information about user roles and passwords for each user in a domain.

🖓 Note

Each domain can have only one management service.

Key features

Key features provided by the management service are:

- Centralized repository for all management information.
- Centralized collection of event logging information.
- Persistent storage of event log and agent information.
- Load management gateway plugins (for example, an SNMP plugin).
- Capability to terminate server processes.

For more detailed information, see Management Service Configuration.

Orbix Configuration Explorer

The Orbix Configuration Explorer is an intuitive Java GUI that enables you to view, modify, and search for configuration settings.

In Figure 4, the **Contents** pane on the left shows the configuration scopes and namespaces displayed for a domain named <code>my-domain</code>. The **Details** pane on the right displays the configuration variables and their values. Clicking on a icon on the left displays its associated variables on the right.

Figure 4 Orbix Configuration Explorer

omain <u>E</u> dit <u>H</u> elp			
	٩		
ntents	Details		
Domains	Name	Value	IDL Type
- 🔚 sample-domain	LOCAL_EVENT_LOG_LOG_FILE	C:\Orbixdata\var\sample-domain\logs\event_log.log	string
– 🥏 IPAC_ORB – 🧭 iona services	LOCAL_NOTIFY_DB_HOME	C:\Orbixdata\var\sample-domain\dbs\notify	string
- Ø IT_MgmtORB	LOCAL_NOTIFY_LOG_DB_HOME	C:\Orbixdata\var\sample-domain\dbs\notify_log	string
- 🥥 IPAC_UTIL	LOCAL_NOTIFY_LOG_LOG_FILE	C:\Orbixdata\var\sample-domain\logs\notify_log.log	string
– 🥏 intfrep_idl_be	MANAGEMENT_CLASSPATH	C:\Orbixdata\etc\domains\sample-domain;C:\Orbixdata\	string
— 🧰 bus — 🧰 plugins	IT_LocatorReplicas	iona_services.locator.NWB-DUNCANH7=corbaloc:iiop:	sequence
- initial_references	LOCAL_EVENT_LOG_DB_HOME	C:\Orbixdata\var\sample-domain\dbs\event_log	string
– 🧰 service	LOCAL_NOTIFY_LOG_FILE	C:\Orbixdata\var\sample-domain\logs\notify.log	string
- 🛅 url_protocols - 🛅 binding	LOCAL_BASIC_LOG_DB_HOME	C:\Orbixdata\var\sample-domain\dbs\basic_log	string
 binuing value_factories 	orb_plugins	local_log_stream,iiop_profile,giop,iiop	sequence
— 🛅 load_balancers	TRADER_LOG	C:\Orbixdata\var\sample-domain\logs\trader.log	string
- 📄 url_resolvers	TRADER_DB	C:\Orbixdata\var\sample-domain\dbs\trader	string
🗆 🧰 policies	LOCAL_BASIC_LOG_LOG_FILE	C:\Orbixdata\var\sample-domain\logs\basic_log.log	string
	admin_plugins	locator_adm,config_adm,ns_adm,nsog_adm,pssdb_a	sequence
	LOCAL_IFR_DB_HOME	C:\Orbixdata\var\sample-domain\dbs\ifr	string
	LOCAL_EVENT_LOG_FILE	C:\Orbixdata\var\sample-domain\logs\event.log	string
	admin_parser_name	admin_parser.tcl	string
	IT_NameServiceReplicas	iona_services.naming.NWB-DUNCANH7=IOR:0100000	sequence
	TRADER_CLASSPATH	C:\PROGRA~1\MICROF~1\Orbix\asp\6.3\lib\trader.jar;C:\	string
	LOCAL NODE DAEMON REFERENCE	IOR:0100000210000049444c3a49545f4e6f6465446	string

Multiple Domains

You can use a single instance of the Orbix Configuration Explorer to manage configuration of multiple domains, both locally and on remote host machines. The Orbix Configuration Explorer communicates with CFRs in any domains that it can contact. It can also read file-based domains where they are locally visible.

Orbix Configuration Explorer architecture

Figure 5 shows an Orbix Configuration Explorer architecture. Orbix Configuration Explorer 1 interacts with both a shared CFR-based domain and a local file-based domain, and can therefore manage configuration in either domain. Orbix Configuration Explorer 2 only manages the CFR-based domain.

Figure 5 Orbix Configuration Explorer Architecture



Orbix Configuration Authority

The Orbix Configuration Authority displays text descriptions of all Orbix configuration settings. Its web browser interface enables you to navigate to and search for configuration information, as shown in Figure 5.

The navigation tree, on the left of the screen displays a hierarchical list of configuration namespaces and variables. The details pane, on the right, displays information about the configuration variables associated with the selected node on the tree.

Figure 6 Orbix Configuration Authority

Child Configuration Authority - Mi Ele Edit View Go Bookmarks (Car • 🛶 • 🚭 🕓 🕎 [Cooks Help	≤■_ ○ ■ ● ● ● ●
🌪 Getting Started 🔂 Labest Headlines		
Orbix Confi	guration Author	ity
Configuration Autho	rity	Help. Search
🖬 - 🔁 stynice		
target_secure_invocatio	Configuration Variable	Description
veti known addressing veti known addressing veti known addressing veti known addressing veti known addression veti known addression	policies: ziop: compression_enabled	compression_enabled specifies whether to enable compression. The default value is true: poicies:ziop.compression_enabled = "true";
formeression threat formeression threat formeression in formeression in formeression in		This means that even when this entry does not appear in configuration, compression is enabled. However, the ziop plug-in must first be loaded in the orb_plugins list, and selected by a server or client binding.
toto: percenter policy follow forwards policy max chain length policy we mechanism	policies: ziop: compression_threshold	compression_threshold specifies the minimum message size that is compressed.
📕 🖬 non tx taraet policy 💌		For example: policies:ziop:compression_threshold =
lone		summer:53186 🛅

The **Search** box located at the top right of the screen enables you to search for information about configuration variables containing a specified text string.

For more detailed information about the Orbix Configuration Authority, see Finding Configuration Information.

Orbix Management Tasks

Typical Orbix management tasks that you can perform include:

- Managing domains.
- Managing servers.
- Monitoring events.
- Managing configuration settings.
- Getting started

This section gives a quick overview of these tasks, and shows where you can find further information in this book.

Managing domains

Typical domain management tasks include:

- Viewing domains.
- Monitoring domain status (whether it is running or stopped).

Managing Applications in the Web Console explains how to manage domains using the Administrator Web Console.

Managing servers

Typical server management tasks include:

- Viewing servers.
- Monitoring server status (whether it is running or inactive).
- Controlling servers (shutting down, setting attributes, and invoking operations).

Managing Applications in the Web Console explains how to manage servers using the Administrator Web Console.

Monitoring events

Typical event management tasks include:

- Selecting a domain in which to manage events.
- Viewing full details of an event.
- Setting event viewing options. For example, you can set the number of events viewed, set the kind of events viewed.

Managing Events in the Web Console explains how to manage events using the Administrator Web Console.

Managing configuration settings

Typical configuration management tasks include:

- Loading up a domain
- Viewing configuration settings
- Searching your configuration
- Finding text descriptions of configuration variables.

Finding Configuration Information explains how to find text descriptions of configuration variables using the Orbix Configuration Authority. Managing Configuration Settings explains how to manage configuration settings using the Orbix Configuration Explorer. Management Service Configuration explains how to manage configuration settings for the management service.

Getting started

For details of getting started with the Administrator Web Console, see Getting Started with the Web Console.

Getting Started with the Web Console

This section explains how to get started with the Administrator Web Console. It describes how to start and navigate through the web console, and how to get help,

The Administrator Web Console is a standard web browser interface that enables you to explore and manage distributed applications. The Administrator Web Console uses HTML to create a standard explorer view to represent the data. For an overview of the Administrator Web Console, see Introduction to Orbix Management.

Note

The Administrator Web Console, Orbix Management Service and Orbix Configuration Explorer are no longer automatically installed. They are available as an optional component. To install, please download and extract the GUI components archive and follow the installation instructions.

The GUI components archive can be downloaded from our Software License & Download (SLD) site.

The GUI components have been separated from the product as they do not fully comply with the Section 508 and WCAG accessibility requirements and guidelines. It is intended that future product releases will include updated GUI components that comply with the relevant accessibility guidelines.

Before Starting the Web Console

This section explains the requirements for starting the web console. Before starting, you should:

- 1. Check your browser version.
- 2. Ensure your configuration is correct.
- 3. Ensure your managed server is running.

Check your browser version

The recommended web browsers for use with the web console are:

- Microsoft Internet Explorer 5.5 or later.
- Mozilla Firefox 1.0 or later.
- Google Chrome 1.0 or later.

Note

Older versions, or other browsers with similar support for JavaScript, can also be used. However, some visual aids may not be available.

Ensure your configuration is correct

When you have successfully installed and configured Orbix, your system is configured to run the Administrator Web Console.

To ensure that your system is configured correctly, type the following command:

install-dir\etc\bin\domain-name_env

Ensure Orbix services are running

Before starting the Administrator Web Console, you must ensure that your Orbix services are running.

To run your Orbix services, use the following command:

```
install-dir\etc\bin\start_domain-name_services
```

Ensure your managed server is running

Administrator enables *runtime* management. This means that any additional instrumented server that you wish to manage (other than the Orbix services) must also be running.

Starting the Web Console

This section describes how to start the web console from your web browser, and how to log in as an administrator. It includes the following:

- Starting in a non-secure domain.
- Starting in a secure domain.
- Troubleshooting the web console.
- Logging into a non-secure domain.
- Logging into a secure domain.

Starting in a non-secure domain

To start the Administrator Web Console, type the following URL in the Address field of your browser:

http://localhost:53185/admin

You can start the web console by specifying the address of any management service host in your browser. To start the web console, use the following URL:

http://host:port_number/admin

The variable host is the name or IP address of the host that the domain's management service is running. The variable port_number is the port number of the web server configured for this domain. The default port number is 53185.

Example addresses are:

```
http://localhost:53185/admin
http://hamlet.myco.com:53185/admin
http://192.165.146.12:53185/admin
```

Starting in a secure domain

To start the Administrator Web Console in a secure (Orbix Security Framework) domain, type the following URL in the **Address** field of your browser:

https://localhost:53186/admin

Accessing the web console over https provides an extra level of security. If you deploy a domain that is either secure or semi-secure, the deployer adds configuration to allow the web console to be accessed over a secure https connection.

Troubleshooting the web console

```
non-secure domain
```

The management service requires the following configuration setting:

```
iona_services{
management{
     policies:well_known_addressing_policy:http:addr_list = ["my-host:
53185", "localhost:53185"];
};
};
```

The variable my-host refers to your hostname.

secure domain

The equivalent setting is as follows:

```
iona_services{
management {
    policies:well_known_addressing_policy:https:addr_list =
["my-host:53186"];
};
};
```

In this case, you would direct your browser to:

https://my-host:53186

The login dialog

When you start up the Administrator Web Console, the **Enter Network Password** dialog appears. This dialog is shown in Figure 7.

Figure 7 The Login Dialog

Enter Netw	vork Passwor	d	? ×
? >	Please type yo	our user name and password.	
IJ	Site:	localhost	
	Realm	IONA Administrator	
	<u>U</u> ser Name	Administrator	
	<u>P</u> assword	****	
	$\overline{\mathbf{V}}$ Save this p	password in your password list	
		OK Can	cel

Logging into a non-secure domain

To log into a domain that does not use the Orbix Security Framework, perform the following steps:

Step	Action
1	In the User Name field, type Administrator.
2	In the Password field, type IONA .
3	Press the OK button.

Note

The User Name and Password are case sensitive.

Logging into a secure domain

When logging into an Orbix Security Framework domain, the user name and password are authenticated against the Orbix Security Framework server. If this server is installed to use the default file system provider, perform the following steps:

Step	Action
1	In the User Name field, type:
	Administrator (for domains created with Orbix 6.3 Service Pack 1 or more recent releases)
	or
	IONAAdmin (for existing, pre-Service Pack 1 domains)
2	In the Password field, type:
	IONA (for domains created with Orbix 6.3 Service Pack 1 or more recent releases)
	or
	admin (for existing, pre-Service Pack 1 domains)

Step	Action
3	Press the OK button.
♀ Note	
The User Name and Password are case sensitive.	

The Administrator Web Console

When you have logged in, the Administrator Web Console appears in a browser window, as shown in Figure 8.

Figure 8 Administrator Web Console



Navigating the Web Console

Navigating through the Administrator Web Console is straightforward. The main components of the console are:

- Navigation tree.
- Details pane.
- Toolbar icons.

This section describes how to use these components to navigate through the system.

The navigation tree

The navigation tree on the left of the console is the starting point for exploring distributed applications. It enables you to navigate to the managed servers that you require.

In Figure 9, the navigation tree displays some managed services.

Figure 9 The Navigation Tree

😑 💩 secure-sample-domain
🗄 💩 iona_services.otstm.summer
🗄 💩 Management Server
🗉 💩 iona_services.locator.summer
🗉 💩 iona_services.node_daemon.summer
🗉 💩 iona_services.naming.summer

Tree nodes

Clicking on any node in the navigation tree causes the contents of the node to be displayed in the details pane on the right of the console. Nodes that use the following icon represent *information types*:

Figure 10 Information Type Icon

ቆ

Information type nodes do not represent manageable objects themselves but indicate the type of the managed objects that they contain. For example, a domain contains a node labeled Servers, and everything contained in this node is a server. A server is defined as a replicated set of processes. For example, under the Servers node is a server instance called web_services.container. This contains a Processes node, which indicates the set of processes that make up this server. This node contains the actual instances of processes within this server, in this case there is only one.

Viewing tree node details

The details pane on the right of the console window shows the details of the selected tree node. Figure 11 shows details for the naming service.

Figure 11 The Details Pane

secure-sample- domain:type=Server,name≕iona_services.naming.summer,Domain≃secur sample-domain		
Attribute	Value	
Name	iona_services.naming.summer	
	iona_services.naming.summer secure-sample-domain	
Name Domain ActiveProcesses		

Viewing the contents of selected nodes

To view the contents of the selected tree node, simply click the node in the navigation tree. This displays the contents in the details pane on the right. As long as there are child nodes in the tree, this display shows a list of the contained child nodes.

Viewing attributes of managed servers

To drill down further into a managed server, click any of the hyperlinks in the **Value** column in the details pane. The hyperlinks in the **Attribute** column show detailed information about the attribute. Figure 12 shows the information displayed for a ActiveProcesses attribute.

Figure 12 Viewing Attributes of Managed Servers



Refreshing the details pane

To perform a forced refresh on the details pane, use the **Refresh** button on the toolbar, as shown in Figure 13:

Figure 13 Refresh Button

¢,

Note

Performing a forced refresh overrides any browser caching. Browser caching should always be disabled when using the Administrator Web Console.

Launching a new window

To launch another instance of the web console, click the #fig_d972e1_d973e1_d974e1_d975e1_d976e1_d977e1

Figure 14 New Window Button

Ť

Launching another instance of the web console is very useful when you want to display multiple managed servers simultaneously.

Administrator Web Console Icons

This section explains the icons used in the Administrator Web Console:

- Toolbar icons.
- Managed server icons.

Toolbar icons

The icons used in the web console toolbar are:

Table 1: Toolbar Icons

Icon	Description
	New Window
	Opens a new browser window that runs the Administrator Web Console independently from the current window.

Description
Refresh
Performs a refresh on the Details Pane . This refresh overrides caching.
Backward
Brings you to the previously viewed page.
Forward
Reverses a Backward move.
Events Console
Displays the Events Console in a separate window.
Quick Overview Help
Displays the quick help in the Details pane.

Managed server icons

The managed server icons are shown in Table 2:

Table 2: Managed Server Icons

Icon	Description
٦	Orbix managed server object.
â	Information type (for example, Servers or Processes).
٦	Orbix managed server process.
\$	Orbix ORB (Object Request Broker).
<u>i</u>	Orbix POA (Portable Object Adapter).

Icon	Description
\$\$. 	Container.
٥	EJB module.
®	Stateless or stateful session bean.
§	Container or bean managed entity bean.
گة	Web module.
遼	Servlet.
•	Data source.
, (1	Resource.
Han I	Namespace.

Managing Applications in the Web Console

This section explains how to use the Administrator Web Console to monitor and control applications in a domain.

The Administrator Web Console displays the manageable components of distributed applications in a single domain. You can use the Administrator Web Console to manage servers within a domain.

Monitoring Managed Applications

This section explains the key concepts and shows how to monitor managed applications in a domain. It includes the following:

- Domains.
- Managed servers and processes.
- Management instrumentation.
- Enabling default instrumentation.
- MBeans.
- Viewing managed servers.
- Attributes of managed servers.
- Drilling into a managed server.
- Monitoring status.

Domains

A *domain* is an abstract grouping of components of a distributed application. Typically a domain describes all the components that run on hosts within the same physical location, whether this is the same LAN, the same building, the same town, or the same country.

A domain can contain any number of managed servers. A managed server can be an instance of an EJB application server, or any other registered process.

⊘ Note

A domain is equivalent to an Orbix configuration domain.

Managed servers and processes

A *managed server* is a set of replicated managed processes. A managed process is a physical process which contains an ORB and which has loaded the management plugin. The managed server can be an EJB application server, CORBA server, or any other instrumented server that can be managed by Administrator. A domain can contain any number and any types of managed servers.

Management instrumentation

A server process becomes a managed server when it contains core management *instrumentation*. This consists of instructions in the server code that enables management of specific server components.

Developers should see the *Orbix Management Programmer's Guide* for details of how to add custom management instrumentation to a server application.

Enabling default instrumentation

By enabling the default management instrumentation on your server, you can display server information in the Administrator Web Console, without adding any custom instrumentation code.

To enable the default instrumentation for your server, set the following configuration variables:

```
plugins:orb:is_managed = true;
plugins:it_mgmt:managed_server_id:name = your_server_name;
```

Set your_server_name to the server name that you want to appear in the Administrator Web Console.

MBeans

An *MBean* is a term used by Java Management eXtensions (JMX) to describe a generic manageable object, a *managed bean*. MBeans are identified by a unique name and can have a number of manageable attributes and operations. All managed entities within a domain are represented by JMX MBeans.

The *Process MBean* is the starting point for navigation through a sever in the Administrator Web Console (iona_services.otstm.summer in Figure 15). It is the first-level MBean that is exposed for management of an application.

Viewing managed servers

You always start monitoring a managed server by selecting it from the navigation tree. Figure 15 shows the initial display for an Object Transaction Service (OTS) managed service.

Figure 15 Viewing a Managed Server in the Web Console



Attributes of managed servers

The details pane on the right of the screen shows the attributes of the managed entity represented by the Process MBean. The grey background of the attribute value cells indicate that all attributes are read-only.

A white text box or a drop down list for the attribute value indicates that an attributed can be modified. For more information, see <u>Setting attributes</u>.

Drilling into a managed server

Attribute values that are represented by a hyperlink indicate a reference to other managed entities. For example, Figure 15, shows a reference to the iona_services.otstm active process).

Click an icon or hyperlink to open the referenced managed entity. This is also known as *drilling into a managed server*. When you drill into a managed server, each managed entity shows its attributes, and the navigation tree is populated. Figure 16 on page 28 shows the results of drilling into the managed server down to its managed EventLog).

Monitoring status

You can use the Administrator Web Console to monitor and control the status of managed servers and domains (for example, to monitor whether a server is active or inactive).

Monitoring status other than status attributes exposed by MBeans is not currently supported by the Administrator Web Console.

Controlling Managed Servers

Controlling a managed server means the ability modify its attributes, and invoke operations on it. This section includes the following:

- Managed server attributes
- Setting attributes
- Example server attributes
- Managed server operations
- Example operations
- Invoking operations
- Shutting down servers
Managed server attributes

You can set attributes in the details pane of the currently displayed managed entity. A text box for the attribute value or a drop-down list indicates that an attribute can be modified. You can get more information on the attribute by clicking on the attribute name in the **Attribute** column.

Setting attributes

To set an attribute, perform the following steps:

Step	Action
1	Select the value field on the right hand side of the details pane (for example, the Filters field in Figure 16).
2	Enter the new value in the text field. Alternatively, for drop-down lists, click the arrow to select one of the values from the list.
3	Click the Set button to apply your changes. You can make changes to multiple attribute values before applying them.

To revert back to the currently active values, click the **Reset** button.

Example server attributes

Figure 16 shows some example attributes for a managed **EventLog**.

Figure 16 Setting Attributes in the Web Console

🚈 IONA Administrator - Microsoft Internet Ex	plorer			
Eile Edit View Favorites Iools Help				
年 Back 🔹 🔿 🗸 🙆 🚮 🥘 Search 🚡	Favorites 🛞 Media 🎯 民)• 4 🖬 🗄		
Address 🔄 http://summer:53185/admin/index.do		Links »		
🏝 💁 🖋 😵 🏤				
Amagement Server Amagement Server	event log managed er EventLog DefaultDomain:type=I	ntity EventLog,orb=iona_services.otstm,name=EventLog,cascaded=iona_services.otstm.summer		
⊞ â iona_services.locator.summer B â iona_services.ifr	Attribute	Value		
 iona_services.otstm.summer iona_services.otstm.summer 	DefaultFilterConfigured	false		
a Encina Transaction Manager	DefaultFilters	["*=WARN[ERROR FATAL"]		
iona_services.otstm 🎄 Workqueue_0	<u>Filters</u>	[["IT_OTS_SRV=*"]		
💩 EventLog ⊞ 🂩 iona_services.event.summer		Set Reset		
	Operation	Parameters		
	viewLog Invoke	none		
EventLog		Eccal intranet		

Managed server operations

Managed servers can expose one or more operations to the management system. You can then invoke these operations from the console. Operations are represented in the details pane by the following:

- Operation name.
- Invoke button.
- Input parameter types.
- Return parameter type.

Example operations

Figure 17 shows an example operation for the **Encina Transaction Manager**. The **Dump** operation takes a transaction log filename as input and returns the contents of the file.

Figure 17 Example Operation in the W	eb Console
--------------------------------------	------------

Operation	Parameters	
Dump Invoke	File Overwrite false 💌 : java.lang.Boolean	: java.lang.String

Invoking operations

Step	Action
1	If the operation takes parameters, type your chosen parameters in the Parameters text box in the details pane. Operations can take a single parameter, multiple, or no parameters.
2	Click the Invoke button in the details pane. Figure 18 shows the dialog displayed for the Update operation.

To invoke an operation, perform the following steps:

Figure 18 Invoking an Operation



Shutting down servers

You can shut down any managed server in the console by performing the following steps:

Step	Action
1	In the Administrator navigation tree, select the server that you wish to shut down. In Figure 18, this is the OTS transaction service.
2	In the details pane, click the Invoke button for the shutdown operation, as shown in Figure 18.

This shuts down the server, and it will no longer be displayed in the **Administrator Web Console**.

Figure 19 Shutdown Operation

IONA Administrator - Microsoft Internet Ex Ele Edit View Favorites Lools Help → Back → → ◇ ③ ④ △ ○ △ ○ Search ④ Address ← http://summer:53185/admin/index.do ★ 1 ● ● ● ● ● ● ● ● ● ● ● ● ● ●		Links »
 		d Object Prvices.otstm.summer re=Server,name=iona_services.otstm.summer,Domain=my-domain Value
🗄 💩 iona_services.otstm.summer	Name	iona_services.otstm.summer
🗄 💩 iona_services.event.summer	 Domain	my-domain
	ActiveProcesses	{ iona_services.otstm.summer }
	<u>State</u>	Running
	Operation	Parameters
	shutdown Invoke	none
🝯 Servers		📃 📄 🛗 Local intranet 🏼 🎢

Managing the ORB Core

For many managed servers, you can view their managed ORBs in the navigation tree of the Administrator Web Console. This section explains how to manage various ORB core information. It includes the following:

- Monitoring the server load
- Server load attributes
- Sampling throughput between invocations
- Managing server logging
- Viewing an event log
- Modifying logging filters

Monitoring the server load

It is important for administrators to know what kind of load key services are under. There are many possible ways of estimating the load on a server, but two key indicators are:

- the number of threads used by the ORB's automatic work queues.
- the request throughput of the ORB.

You can view this information by clicking on the ORB MBean below the managed process in the navigation tree, as shown in Figure 20.

Server load attributes

The attributes displayed for the server load include the following:

Number of threads.

You can view the number of threads that the ORB is currently using in all of its automatic work queues using the TotalNumberOfThreadsInUse attribute. This gives an instantaneous snapshot of the number of threads in use.

Thread pool size.

Thread pools grow to meet demand and then shrink as demand for threads reduces. The TotalThreadPoolSize attribute is therefore a reflection of recent demands on the thread pool.

Thread queue length.

The TotalQueueLength is an indication of the number of items waiting to be serviced by a thread.

Request throughput.

The IncomingRequests attribute shows the number of requests initiated on the ORB. The OutgoingRequests shows number of requests initiated by the ORB. Refreshing the display enables you to monitor differences in these values, however, it can be difficult to estimate what this means in throughput terms.

Figure 20 Server Load Details

IONA Administrator - Microsoft Internet Ex File Edit View Favorites Tools Help	xplorer			
Gie galt gen rgreines gees gep	🗟 Favorites 🕼 Media 🏼 🖓 🗟 🗸 🛋 🛒			
Address Ad		Links ²		
	C++ ORB iona_services.naming DefaultDomain:type=ORB,name=iona_services.naming,cascaded=iona_services.naming.summer			
ao NameService ⊞ 🕵 iona_services.naming	Attribute	Value		
🗄 💩 iona_services.locator.summer	ORBName	iona_services.naming		
	ORBId	iona_services.naming		
	<u>Plugins</u>	{ it_mgmt, local_log_stream, codeset, iiop_profile, giop, ots, atli2_ip, iiop, poa, pss_db, ots_lite }		
	TotalNumberofAutomaticWorkQueues	2		
	TotalThreadPoolSize	6		
	TotalNumberofThreadsInUse	5		
	TotalQueueLength	0		
	OutgoingRequests	33		
	IncomingRequests	33		
	SamplingInterval	0		
	IncomingRequestThroughput	0		
	SamplePeriodBegan	Thu, 16 Dec 2004 11:31:33.1280000		
	SamplePeriodEnded	Thu, 16 Dec 2004 11:31:33.1280000		
	Operation Parameters			
	Update Invoke			
() 8		Cocal intranet		

Sampling throughput between invocations

You can use the **Update** operation to sample the throughput between subsequent invocations. For example, click **Update**, wait for a few seconds, and click **Update** again. The IncomingRequestThroughput parameter will indicate the rate of requests per second processed in the interval between the two calls (rounded to the nearest whole number).

The SamplingInterval attribute records the length of the sampling period in milliseconds; while the SamplePeriodBegan and SamplePeriodEnded attributes indicate respectively when the sample period began and ended.

Managing server logging

For Java and C++ servers, the ORB's event log is instrumented. The **EventLog** MBean is displayed in the navigation tree as a child of the ORB MBean, as shown in Figure 21. This enables you to perform the following tasks:

- View the event log.
- Modify the logging filters.

Figure 21 The Event Log

🗿 IONA Administrator - Microsoft Internet Explorer				
File Edit View Favorites Tools Help				
🗢 Back 🔹 🤿 🖌 🙆 🕼 🥘 Search 👔	Favorites 🛞 Media 🎯 民	y- 🗿 🖬 🗐		
Address Addres		✓ Links ≫		
🏝 i 🙆 i 🖋 i 😵 i 🏤				
	event log managed er EventLog DefaultDomain:type=I	tity EventLog,orb=iona_services.otstm,name=EventLog,cascaded=iona_services.otstm.summer		
🗄 💩 iona_services.ifr	Attribute	Value		
iona_services.otstm.summer	DefaultFilterConfigured	false		
at Encina Transaction Manager	DefaultFilters	["*=WARNJERRORJFATAL"]		
 Kiona_services.otstm Workqueue_0 EventLog iona_services.event.summer 	<u>Filters</u>	[["IT_OTS_SRV=*"]		
		Set Reset		
	Operation	Parameters		
	viewLog Invoke	none		
4				
🙋 EventLog		🛛 🕅 🗮 Local intranet		

Viewing an event log

To view the event log for a Java or C++ server, perform the following steps:

- 1. In the navigation tree, click the **EventLog** MBean.
- 2. In the details view, click the **viewLog** operation. This displays recent logging events for this ORB. Figure 21 shows a naming service log.
- 3. Click **<Prev** and **Next>** to navigate the log. Clicking **Next** will bring up more recent events). Clicking on **Back to Details** returns you to the main details page for that event log.

Figure 22 The Event Log Viewer

IONA Administrator - Microsoft Internet E: Eile Edit View Favorites Iools Help ← Back • → • ② ② 巯 ◎ 《 Search ④ Address ② http://summer:53185/admin/index.do	-	8• # # B		Links
□ 💁 🖋 🚱 ♠				
 a my-domain a my-domain a my-domain a my-domain a my-domain b my-dom	Log Viewer Back to Details < Prev Next >			
iona_services.naming.summer å NameService	Date-Time	Subsystem	Event	Message
□ X iona_services.naming Workqueue_1	Thu, 16 Dec 2004 11:31:33.0000000	IT_PSS_DB:68	Information	Replication enabled for DB env it_naming_store
أي Workqueue_0 أي EventLog ⊡ أي iona_services.locator.summer	Thu, 16 Dec 2004 11:31:33.0000000	IT_PSS_DB:89	Information	Starting recovery of env it_naming_store
☆ iona_services.ifr ☆ iona_services.otstm.summer ☆ iona_services.event.summer ☆ iona services.event.summer	Thu, 16 Dec 2004 11:31:33.0000000	IT_PSS_DB:39	Information	Opened env it_naming_store
Ima_services.event.summer	Thu, 16 Dec 2004 11:31:33.0000000	IT_PSS_DB:91	Information	Master for DB env it_naming_store started
	Thu, 16 Dec 2004 11:46:33.0000000	IT_PSS_DB:31	Information	checkpoint on env it_naming_store completed successfully
	Thu, 16 Dec 2004 12:01:33.0000000	IT_PSS_DB:31	Information	checkpoint on env it_naming_store completed successfully
	Thu, 16 Dec 2004 12:16:33.000000	IT_PSS_DB:31	Information	checkpoint on env it_naming_store completed successfully
EventLog				🗮 Local intranet

Modifying logging filters

You can change your event log filters dynamically by setting the **Filters** attribute. This applies to both Java and C++ servers. This will have no effect at all if you enter an illegal value. The value must be a list of strings, for example:

```
["IT_ClassLoading=*", "IT_IIOP_TLS=WARN+ERROR+FATAL"]
```

This capability is very useful if your server behaves unexpectedly and you need to turn up the provided level of logging without restarting the server.

Managing Events in the Web Console

This section explains how to use the Administrator Web Console to monitor events. It explains how to start its Events Console, and view events for a domain.

The Administrator Web Console's **Events Console** enables you to view events generated by managed servers. The events console shows an up-to-date list of events in reverse chronological order. You can customize the severity of events and apply filters to selectively view events.

Starting the Events Console

This section explains how to start the Administrator Web Console's Events Console.

Using the Events Button

To start the **Events Console**, click the **Events** button in the Administrator Web Console toolbar, as shown in Figure 23.

Figure 23 Events Button

ø

If an events console is already open, subsequent clicks on this button bring the web console to the foreground.

Example Events Console

An example **Events Console** started from the web console is shown in Figure 24. The events are shown in a list starting with the most recent event at the top.

Figure 24 Events Console

🔁 Thre	eshold:	Info	•	Display <mark>50 </mark>	
Date	Time		Severity	Event Source	Event Name
12/16/04	11:31	AM	Info	Management Server	JMX.mbean.registered
12/16/04	11:31	AM	Info	Management Server	JMX.mbean.registered
12/16/04	11:31	AM	Info	iona_services.management.server	com.iona.management.ProcessRegistered
12/16/04	11:31	AM	Info	Management Server	JMX.mbean.registered
12/16/04	11:31	AM	Info	Management Server	JMX.mbean.registered
12/16/04	11:31	AM	Info	Management Server	JMX.mbean.registered
12/16/04	11:31	AM	Info	iona_services.management.server	com.iona.management.ProcessRegistered
12/16/04	11:31	AM	Info	Management Server	JMX.mbean.registered
12/16/04	11:31	AM	Info	Management Server	JMX.mbean.registered
12/16/04	11:31	AM	Info	Management Server	JMX.mbean.registered
12/16/04	11:31	AM	Info	iona_services.management.server	com.iona.management.ProcessRegistered
12/16/04	11:31	AM	Info	Management Server	JMX.mbean.registered
12/16/04	11:31	AM	Info	Management Server	JMX.mbean.registered
12/16/04	11:31	AM	Info	Management Server	JMX.mbean.registered
12/16/04	11:31	AM	Info	iona_services.management.server	com.iona.management.ProcessRegistered
12/16/04	11.21	ΔМ	Info	Manadomont Sorver	IMX mbean registered

Viewing Events

This section explains how to use the Administrator Events Console. It includes the following:

- Viewing Events in a Domain
- Refreshing the Event List
- Setting the Number of Events Displayed
- Setting the Event Threshold
- Information Displayed in the Event List
- Viewing Full Details of an Event
- Filtering Events

Viewing Events in a Domain

Events are always shown on a per-domain basis. To view events from a different domain, start a web console connecting to the domain's management service and launch the events console from there. See Before Starting the Web Console for more details.

Refreshing the Event List

The event display shows an up-to-date list of events when first started. The display is not updated automatically. To refresh the display, click the **Refresh** button in the toolbar, as shown in Figure 25.

Figure 25 Refresh Button

¢,

Setting the Number of Events Displayed

To set the maximum number of events being retrieved from the management server, click the dropdown box at the **Display Events** field at the top of the console.

Setting the Event Threshold

The **Threshold** setting specifies the lowest severity of events that you want to include in the displayed list. There are four severities:

• Critical

Error

Warning

Info

The highest event severity is Critical and the lowest is Info.

To set the events threshold, click the **Threshold** drop-down box at the top left of the console.

Information Displayed in the Event List

The event list shows the following summary information about each event:

- Date and time of the event.
- Severity of the event.
- Agent that created the event.
- Name of the event.

Viewing Full Details of an Event

To get comprehensive details of a particular event, simply click the event in the event list. Figure 26 shows displays full details for a an event from an example Bank application. This application sends a ManagediBankAuthorisation.loginFailed event when a user login fails.

Filtering Events

You can also customize the severity of events and apply filters to selectively view events by modifying **shared** filters for a domain. For more information, see Management Service Configuration.

Figure 26 Full Details of an Event

Microsoft	Internet Explorer	×
	Event Name: ManagediBankAuthorization.loginFailed Severity: Info Timestamp: Wed May 16 18:20:23 GMT+01:00 2001 Sequence Number: 404	
	Source Agent: iPAS.Server.Default Source MBean: examples.ejb.management.ibank.ManagediBankAuthorization@2d81	l3e
	Event Description: Attempt to log into account FAILED for username: john	
	Properties: Message: Attempt to log into account FAILED for username: john Type: ManagediBankAuthorization.loginFailed TimeStamp: 990033623222 SequenceNumber: 0 Source: examples.ejb.management.ibank.ManagediBankAuthorization@2d813e UserData: null	
	(OK)	

Management Service Configuration

This section explains how the Orbix management service gets its configuration, and shows an example in the Orbix Configuration Explorer.

You can configure the Orbix management service by directly editing your configuration file. Configuration files are stored in the install-dir/etc/domains directory

Management service scope

The management service gets its configuration from the iona_services:management configuration scope in your configuration file.

If the configuration variables in the iona_services:management scope are not configured correctly, the management service starts up, and sends warnings to the event log and standard error. Depending on the particular variable, a default value is used, or the feature is not enabled (for example, if a persistent filename is not configured, persistent storage is not enabled).

Example configuration file

The following extract from a configuration file shows example configuration variables in the iona_services:management SCOPE:

```
management
{
    event_log:filters=["IT_MGMT_SVC=INFO_HI,WARN,ERR,FATAL"];
plugins:local_log_stream:filename =
    "install-dir/var/domain-name/logs/mgmt_svc.log";
    .
    .
    .
    .
    .
    .
};
```

This section explains how to use the iona_services:management variables to configure management service features.

Orbix Configuration Explorer example

Figure 41 shows management configuration variables in the Orbix Configuration Explorer.

For information about how to use the Orbix Configuration Explorer to manage configuration variables, see Managing Configuration Settings.

Figure 41 Orbix Configuration Explorer

<u>D</u> omain <u>E</u> dit <u>H</u> elp				
Contents		Details		
locator		Name	Value	IDL Type
📕 🚽 🥏 otstm		ping_interval	10	string
event		idle_period	600	string
📄 🥏 🥏 management		persistent_filename	f:\orbix\var\my-domain\d	string
policies			1	
event_listener				
- initial_references				
event_processor				
event_barrier				
agent_container	-			
— 📄 severity_assigner				
- in web_server				
snmp_trap				
│				
- binding				
event_log				
event_history				
	-			
Ready				
Configuration				

Configuring the Event Log

This section explains how to enable the event log for management service events, and how to send the event log output to a file.

Configuring the event log filter

To enable event logging for the management service, you must set the required event severities for the IT_MGMT_SVC subsystem. You can specify these event severities using the event_log_filters configuration variable in the iona_services:management configuration scope.

The following example shows a recommended default setting in a configuration file:

```
event_log:filters="{IT_MGMT_SVC=INF0_HI+WARN+ERROR+FATAL}";
```

The following setting enables logging for all management service events:

```
event_log:filters = "{IT_MGMT_SVC=*}";
```

Sending the log output to a file

By default, Orbix logs event messages to a file. To change the location of this file, update the following variable in the iona_services:management configuration scope:

```
plugins:local_log_stream:filename =
"install-dir/var/domain-name/logs/mgmt_svc.log"
```

Configuring the local log stream

When running the management service, if the configured log file does not appear, you might need to add the local_log_stream plugin to the orb_plugins variable. For example:

```
orb_plugins = ["local_log_stream", "iiop_profile", "giop", "iiop", "ots"];
```

These configuration variables must be set correctly in order for the management service to write to the event log file.

Configuring Resource Agents

This section describes how to configure resource agent files and resource agent timeouts for the management service.

You must set all configuration variables for the management service in the management configuration scope.

Resource agents

Managed server applications register a resource agent reference with the management service. This enables a managed server to be made available for management. Resource agent references are stored in your file system.

A resource agent is an interface to a JMX instrumentation plugin in a managed server. A resource agent is loaded into a managed server to export server MBean information to the management service and management consoles. A resource agent is the sole entry point into a managed server.

Resource agents are registered with the management service, using a unique name, when they are loaded. Resource agents normally unregister when their server terminates; however, abnormal termination can result in references remaining in your system.

Configuring a resource agent file

You can use the following variable to specify the name of the persistent file in which resource agent references are stored:

```
agent_container:persistent_filename =
"install-dir/var/domain-name/mgmt/persistent/agents";
```

If an agents file is not specified (or if the file can not be created) the persistent storage is disabled. This means that a restarted management service does not know about the registered resource agents.

Configuring resource agent timeouts

You can use the following variable to specify the timeout in seconds to wait between repeatedly pinging all agents to verify that they are running:

```
agent_container:ping_interval = "10";
```

You can specify a timeout value of any number greater than **o** seconds. The default value is **1o** seconds.

Configuring Event Listeners

Client applications requesting events from the management service can register an event listener, so that all events are passed to those clients immediately. This section explains how to configure support for event listeners in the management service.

You must set all configuration variables for the management service in the iona_services:management configuration scope.

Configuring an event listener file

Use the following variable to specify the persistent file in which event listener references are stored:

```
event_processor:persistent_filename =
"install-dir/var/domain-name/mgmt/persistent/listeners";
```

If a listeners file is not specified (or if the file can not be created), the persistent storage is disabled. This means that a restarted management service does not know about the registered event listeners.

Configuring an event listener timeout

Use the following variable to specify the timeout in seconds to wait between repeatedly pinging all event listeners to verify that they are running:

```
event_processor:ping_interval = "10";
```

You can specify a timeout value of any number greater than **o** seconds. The default value is **1o** seconds.

Configuring Event History

This section explains how to configure an event history file, the event history memory capacity, and the interval at which event history is purged. You must set all configuration variable values for the management service in the management configuration scope.

Event history

Events received by the management service from managed applications are stored in the file system, so that they can be retrieved later.

You can specify the event history capacity to prevent the system from becoming overloaded. The recommended capacity is 1000 events. You can also specify an interval after which the event history file is purged. The default interval is 10 minutes.

Configuring an event history file

Use the following variable to specify the persistent file in which event history is stored:

```
event_history:persistent_filename = "install-dir/var/domain-name/mgmt/
persistent/events";
```

If an events file is not specified (or if the file can not be created), the persistent storage is disabled.

Configuring event history memory

Use the following variable to specify the number of events that are stored:

```
event_history:memory_capacity = "1000";
```

The default number of events is 1000. The maximum number of events is 4000. You must specify a positive value.

Configuring event history purges

Use the following variable to specify the interval at which the event history is purged:

```
event_history:trim_interval = "600";
```

The default is 600 seconds (10 minutes). You must specify a positive value.

Configuring Event Filters

Client applications requesting events from the management service use a named event filter to maintain their own event severity mapping and event threshold values. This section explains how to specify event severity files, and an event threshold file.

Configuring an event severity file

Use the following variable to specify where event severities are stored in the file system:

```
severity_assigner:persistent_filename = "install-dir/var/domain-name/mgmt/
persistent/severities";
```

The severities file is an internally used archive.

Configuring an event filter threshold file

Use the following variable to specify where event filter thresholds are stored in the file system:

```
event_barrier:persistent_filename = "install-dir/var/domain-name/mgmt/
persistent/threshold";
```

The threshold file is an internally used archive.

Configuring a default event severity file

You can also specify default event severity mapping using a default severity file. The event severities specified in this file apply to all new filters. The default event severity file is a pure text file, containing event name and event severity pairs, for example <code>com.iona.management.testevent 0</code>

Event severities

Valid event severities are represented by integers in the 0...3 range:

0	CRITICAL	
1	ERROR	
2	WARNING	
3	INFO	

Use the following variable to specify where the default event severity file is stored in your file system:

```
severity_assigner:default_filename = "install-dir\var\domain-
name\mgmt\persistent\default_severities.txt";
```

Configuring Event Processing

This section explains how to configure consolidated logging, an idle event period, and a logfile filter.

You must set all configuration variable values for the management service in the iona_services:management configuration scope.

Consolidated logging

Successive events with identical names and property values are treated as identical by a consolidated logging feature. This means that such follow-up events are eliminated and reported collectively at a later time (either after some delay, or before the next different event).

You should leave this consolidated event feature enabled, because it protects the system by reducing event numbers.

Enabling consolidated logging

Use the following variable to control consolidated logging:

```
event_listener:consolidated_logging = "true";
```

The default setting is true.

Configuring an idle event period

Idle event filters are removed and recreated internally in an identical state for further requests only. Use the following variable to specify the number of seconds an event filter is kept alive in memory:

```
event_processor:idle_period = "600";
```

Configuring the logfile filter

The event log contains a human-readable log of all the management events that have passed through the logfile filter (a reserved system filter). The logfile filter is used by the management service to generate tab-separated text files.

Use the following variable to specify where these event log text files are stored in your system:

event_log:filename_base = "install-dir/var/domain-name/mgmt/logs/events";

These filenames are appended with the a timestamp in the standard format .ddMMyyyy. For example: events.08102001

Configuring the Management Service Web Server

The Administrator Web Console serves as a web browser interface for HTTP-based access to the management service. This section shows how to configure the web server for this browser interface.

Configuring the web server

The web server's port number is specified by the web_server:port_number configuration variable in the liona_services:management scope. The default value is 53185. If this variable or port number is not found, the web server is disabled.

Orbix Configuration Explorer example

Figure 42 shows a configuration setting for the web server's port number in the Orbix Configuration Explorer.



Figure 42 Orbix Configuration Explorer Example

Finding Configuration Information

This section explains how to use the Orbix Configuration Authority to find information about Orbix configuration settings.

Orbix Configuration Authority

This section introduces the Orbix Configuration Authority, shown in Figure 27. The Orbix Configuration Authority provides a web browser interface to descriptive information about all Orbix configuration settings. This section includes the following topics:

- Orbix Configuration Authority components
- Orbix Configuration Authority icons

Figure 27 Orbix Configuration Authority

🥹 Orbix Configuration Authority - Mozilla Firefox				
Eile Edit View Go Bookmarks Tools Help				
🗇 • 🗇 • 🥰 🛞 🐔 🚺	https://summer:53186/ca/ca.html	<u>⊜</u> ⊂ ⊙ ⊙		
🐢 Getting Started 🔯 Latest Headlines				
Orbix Config	guration Authori	t y		
Configuration Author	<u>ity</u>	Help Search		
shmiop				
target secure invocatio	Configuration Variable	Description		
well known addressinc ziog compressor for compression enable	policies:ziop:compression_enabled	<i>compression_enabled</i> specifies whether to enable compression. The default value is true: policies:ziop:compression_enabled = "true";		
compression threst compressor id allow unauthenticated certificate constraints ; concertificate constraints ;		This means that even when this entry does not appear in configuration, compression is enabled. However, the ziop plug-in must first be loaded in the orb_plugins list, and selected by a server or client binding.		
follow forwards policy	policies:ziop:compression_threshold	<i>compression_threshold</i> specifies the minimum message size that is compressed. For example:		
		policies:ziop:compression_threshold =		
Done		summer:53186 📋 🥢		

Orbix Configuration Authority components

The Orbix Configuration Authority, as shown in Figure 27, is divided into three main areas.

Navigation tree	The navigation tree, on the left of the screen, is the starting point for exploring for configuration information. This is used to display a hierarchical list of configuration namespaces and variables.
Details pane	The details pane, on the right of the screen, displays information about the configuration variables associated with the selected node on the tree.
Search box	The Search box located at the top right of the screen enables you to search for information about configuration variables containing a specified text string.

Orbix Configuration Authority icons

The icons used in the Orbix Configuration Authority are shown in Table 3.

Table 3: Orbix Configuration Authority Icons.

Icon	Description	
	Configuration namespace.	
Ē	Configuration variable.	

Starting the Orbix Configuration Authority

This section describes how to start the Orbix Configuration Authority from directly from your web browser. It includes the following:

- Starting from your browser.
- Troubleshooting.

```
Note
```

Before starting the Orbix Configuration Authority, check the steps described in Before Starting the Web Console.

Starting from your browser

To start the Orbix Configuration Authority, type the following URL in the **Address** field of your web browser:

http://localhost:53185/ca

You can start the web console by specifying the address of any management service host in your browser. To start the web console, use the following URL:

http://host:port_number /ca

The variable host is the name (or IP address) of the host that the domain's management service is running. The variable port_number is the port number of the management service configured for this domain. The default port number is 53185.

Example addresses are:

```
http://localhost:53185/ca
http://hamlet.myco.com:53185/ca
http://192.165.146.12:53185/ca
```

In a secure domain, the default address is as follows:

```
https://hostname:53186/ca
```

For for more details, see Starting in a secure domain.

Troubleshooting

The management service requires the following configuration setting for the web browser used by the Orbix Configuration Authority:

```
iona_services{
management{
        policies:well_known_addressing_policy:http:addr_list = ["host:port-
number", "localhost:port-number"];
};
};
```

The variable my-host refers to your hostname; port-number refers to the management service port number that is configured for your domain.

Viewing Configuration Information

You can browse for information using the navigation tree and details pane. This section explains the following:

- Viewing for all variables in a namespace
- Viewing for a specified variable
- Searching the Orbix Configuration Authority
- Viewing the entire contents
- Printing a hard copy

Viewing for all variables in a namespace

To view information about all the variables contained in a specific namespace, click the namespace folder in the navigation tree.

This displays text descriptions for all the variables in that namespace in the right pane.

Figure 27 on page 41 shows the information displayed for the variables in the destinations namespace. This is used to configure the Java Messaging Service (JMS).

Viewing for a specified variable

To view information about a particular variable, drill down to the variable icon in the navigation tree. This displays a text description for the variable in the right pane.

Figure 28 shows the information displayed for the Comet:Service:NameService variable. This is used to configure the naming service used to bridge from CORBA to Microsoft COM (Common Object Model).

Figure 28 Viewing a Configuration Variable



Searching the Orbix Configuration Authority

Use the **Search** box in the top right of the screen to search the Orbix Configuration Authority for all variable names that contain your specified search text.

For example, enter the text classloader to find all configuration variable that contain the text classloader in its name.

Viewing the entire contents

To view the entire contents of the Orbix Configuration Authority, press the **Search** button without typing in any search string. This displays all information about all Orbix configuration variables stored in the Orbix Configuration Authority.

Printing a hard copy

Viewing the entire contents of the Orbix Configuration Authority displays all the information in a single HTML file, sorted alphabetically by configuration namespace. You can print the result of for a hard copy of all the information in the Orbix Configuration Authority.

Note

Ensure that your system is configured to print a Landscape orientation before printing the entire contents.

Managing Configuration Settings

This section explains how to use the Orbix Configuration Explorer to manage your Orbix configuration settings in multiple domains.

The Orbix Configuration Explorer enables you to view, search for, and edit configuration settings. For details of how to find information about specific Orbix configuration settings, refer to Finding Configuration Settings. Alternatively, see the *Orbix Configuration Reference*.

Orbix Configuration Explorer

This section introduces the Orbix Configuration Explorer, shown in Figure 29. It includes the following sections:

- Orbix Configuration Explorer components
- Contents pane icons
- Toolbar icons
- Starting Orbix Configuration Explorer

Figure 29 The Configuration View Tab

ntents	Details		
Domains	Name	Value	IDL Type
Estimation	domain	itconfig://IOR:010000002400000	string
– 🥏 demos	orb_plugins	local_log_stream,iiop_profile,gi	sequence
- 🥥 IPAC_ORB - 🥥 IPAC_UTIL	admin_plugins	locator_adm,config_adm,ns_ad	sequence
- Ø kdm_admin	admin_parser_name	admin_parser.tcl	string
— 🥭 IT_MgmtORB	IT_LocatorReplicas	iona_services.locator.summer=	sequence
- 🥥 iona_services	IT_NameServiceReplicas	iona_services.naming.summer	sequence
— 🥥 intfrep_idl_be — 🧭 iona_utilities	itadmin_x509_cert_root	f:\orbix\asp\6.2\etc\tls\x509\certs\	string
- Ø multicast_demo	IT ConfigRepositoryReplicas	iona services.config rep.summ	sequence
 Secure_jms_client COMet binding plugins deployer policies url_protocols url_resolvers load_balancers value_factories initial_references 			

Orbix Configuration Explorer components

The Orbix Configuration Explorer is divided into three main areas.

Contents pane	The Contents pane, on the left of the screen, is the starting point for exploring your configuration. This is used to display a hierarchical list of configuration domains, scopes, and namespaces.
Details pane	The Details pane, on the right of the screen, displays the configuration variables associated with the selected node on the tree, and also enables you to edit these variables. Figure 29 shows a blank pane because a configuration domain has not been loaded yet.

Menu and	The menu and toolbar, located at the top of the screen, enable you to perform
Toolbar	various actions in a domain (for example, searching your configuration, or
	modifying a configuration setting).

⊘ Note

In a file-based domain, you can view and find configuration settings. In a configuration repository domain, you can also create, modify and delete configuration settings.

Contents pane icons

The icons used in the **Contents** pane are shown in Table 4.

Table 4: Navigation Tree Icons.

Icon	Description		
\bigcirc	Unloaded configuration domain.		
-	File-based configuration domain.		
	Configuration repository domain.		
Ø	Configuration scope.		
	Configuration namespace.		

Toolbar icons

The icons used in the Orbix Configuration Explorer toolbar are shown in Table 5.

Table 5: Toolbar Icons.

Icon	Description		
$\overline{\mathcal{O}}$	Create a configuration scope.		
<u>*</u>	Create a configuration namespace.		

Icon	Description
掌中	Create configuration variable.
۹	Find a configuration setting.
8	Delete a configuration setting.
2	Help.

Starting Orbix Configuration Explorer

To start Orbix Configuration Explorer, perform the following steps:

1. Change to the following directory:

```
*install-dir*\asp\*version*\bin\
```

2. Enter the following command:

itconfigexplorer

Viewing Configuration Settings

You can view the contents of a domain using the navigation tree and details pane. This section explains the following:

- Loading up a domain.
- Drilling into the tree.
- Viewing Configuration Variables.

Loading up a domain

Before you can view your configuration settings, you must first load up your selected domain in the navigation tree.

To load up a domain, click the domain in the navigation tree. The domain icon in the navigation tree changes to a loaded domain, and the variables in the root configuration scope are displayed in the details pane.

Figure 30 shows a loaded domain in the navigation tree, and the root level settings for this domain in the **Details** pane. In this case, the domain is a local file-based domain named <code>my-domain</code>.

Viewing Configuration Scopes and Namespaces

You can view configuration scopes and namespaces in a domain by simply expanding or contracting the loaded domain in the navigation tree.

To expand a domain in the tree, click the + sign on the left. You can also double-click a the domain icon to expand it. For example, Figure 30 shows the result of double-clicking on the my-domain icon.

IE IONA Configuration Explorer 6.2				
Domain Edit Help				
Contents	Details			
🞝 Domains	Name	Value	IDL Type	
🖶 🔚 my-domain	OTSTM_BACKUP_RESTAR	f:\orbix\var\my-domain\dbs\	string	
📙 🦳 secure-sample-domain	admin_plugins	locator_adm,config_adm,n	sequence	
	, IT_NameServiceReplicas	iona_services.naming.sum	sequence	
	orb_plugins	local_log_stream,iiop_profi	sequence	
	IT_LocatorReplicas	iona_services.locator.sum	sequence	
	LOCAL_IFR_LOG_FILE	f:\orbix\var\my-domain\logs\i	string	
	LOCAL_COMET_CACHE_F	f:\orbix\var\my-domain\dbs\	string	
	OTSTM_RESTART_FILE	f:\orbix\var\my-domain\dbs\	string	
	OTSTM_INITIAL_DISK_SIZE	2	string	
	LOCAL_NODE_DAEMON	IOR:010000002100000049	string	
	LOCAL_EVENT_LOG_FILE	f:\orbix\var\my-domain\logs\	string	
	LOCAL_IFR_DB_HOME	f:\orbix\var\my-domain\dbs\ifr	string	
	MANAGEMENT_CLASSPATH	f:\orbix\etc\domains\my-do	string	
	admin_parser_name	admin_parser.tcl	string	
	OTSTM_INITIAL_DISK	f:\orbix\var\my-domain\dbs\	string	
Ready				
Configuration				

Figure 30 Viewing Configuration Settings

Drilling into the tree

You can view sub-scopes and sub-namespaces by drilling further into the navigation tree. For example, the navigation tree in Figure 31 shows the contents of the liona_services.management scope.

Collapsing the tree

To close a tree node, click the - sign on the left, or double-click an expanded folder. For example, in Figure 31, double-click my-domain.

IV IONA Configuration Explorer 6.2			
<u>D</u> omain <u>E</u> dit <u>H</u> elp			
Contents	Details		
tevent ▲	Name	Value	IDL Type
	generic_server_plugin	java_server	string
🕀 🥥 server			
– 🗖 policies			
- event_listener			
initial_references			
event_processor			
event_barrier			
remote_objects			
agent_container			
- severity_assigner			
web_server snmp_trap			
- security			
- plugins			
binding			
event_log			
event_history			
L - D url resolvers			
Ready			
Configuration			

Figure 31 Viewing Configuration Scopes and Namespaces

Viewing Configuration Variables

The details pane on the right of the **Configuration View** displays the configuration variables contained directly within the currently selected scope or namespace.

To view a configuration variable in a domain, navigate to its scope or namespace in the navigation tree. The variable details appear in the details pane. For example, Figure 32 displays the variables contained in the event_processor namespace, in the iona_services:management scope. The details pane displays the variable name, value, and IDL type.

ontents			Details		
- 🍎 to	ocator		Name	Value	IDL Type
	tstm		ping_interval	10	string
	vent .		idle_period	600	string
	nanagement Ziserver		persistent_filename	f:\orbix\var\my-domain\d	string
	policies				
	event_listener	1			
	initial_references				
	event_processor	1			
	event_barrier				
	remote_objects				
	agent_container	1			
	severity_assigner] web_server				
	snmp_trap	1			
	security				
	plugins				
	binding				
	event_log				
	event_history				
📃 🦰 🥏 IPAC	ORB	-			

Figure 32 Viewing Configuration Variables
Finding Configuration Settings

This section explains how to find configuration settings in a loaded domain. It includes the following:

- Finding a text string in a domain
- Example search
- Performing repeat searches

For details of how to load up a domain, see Loading up a domain.

Finding a text string in a domain

To search a domain for occurrences of a particular text string, perform the following steps:

Step	Action
1	Select your domain in the navigation tree.
2	Select Edit>Find from the main menu. The Find dialog appears, as shown in Figure 33. Alternatively, click the Find button in the toolbar:
3	Enter your chosen text in the Find text box. Figure 33 shows a search for the string web_server .
4	Press the Find button. Figure 34 shows the result of this search. The web_serv er configuration namespace and its configuration variables are displayed.

Example search

Figure 33 shows an example search in the **Find** dialog.

Figure 33 Example Search

Find	×
?	Find: event_history
	Variable names Variable values
	Match case Match whole words
	Find Cancel

Performing repeat searches

To repeat your last search, select **Edit>Find Again** from the main menu. Alternatively, press the **F3** button.

Figure 34 Result of Example Search

IONA Configuration Explorer 6.2					
Domain Edit Help					
Contents		Details			
📄 🔄 🥏 node_daemon 🦉		Name	Value		IDL Type
🗈 🕀 🥥 locator		trim_interval	60000	string	
📗 📄 💇 otstm		persistent_filename	f:\orbix\var\my-domain\	string	
event		memory_capacity	1000	string	
🔄 🗁 🧭 management				g	
⊕- È policies	ł				
event_listener					
📄 📄 initial_references					
📃 🚽 — 🧰 event_processor	-				
event_barrier					
remote_objects					
agent_container					
- Construction - Cons					
snmp_trap					
- Security					
🕀 🔂 plugins					
binding					
event_log					
event_history	-				
Searching - Variable: server_binding_list					
Configuration					

Modifying Configuration Settings

You can modify the contents of a domain using the navigation tree and details pane. This section explains how to modify configuration variable settings. It includes the following:

- Loading up a domain
- Configuration variable settings
- Modifying configuration variables

Note

You can modify settings in a configuration repository (CFR) domain only. You can not use this tool to modify settings in a file-based domain. You should edit your configuration file instead.

The default configuration settings are suitable for most environments. For detailed information about configuration settings, see Finding Configuration Information.

Loading up a domain

Before you can modify your configuration settings, you must first load up your selected domain in the navigation tree.

To load up a domain, click the domain in the navigation tree. The domain icon in the navigation tree changes to a loaded domain, and the variables in the root configuration scope are displayed in the details pane.

Figure 35 shows a loaded configuration repository domain, named configrep_domain, in the navigation tree. The root level settings for this domain are shown in the details pane.

Note

Your CFR must first be running before it can load up in the Orbix Configuration Explorer.

Figure 35 Loaded Configuration Repository Domain

0 🛐 🍳			
ontents	Details		
🕹 Domains	Name	Value	IDL Type
🦻 🗐 configrep_domain	domain	itconfig://IOR:010000002400000	string
🤵 IPAC_ORB	orb_plugins	local_log_stream,iiop_profile,gi	sequence
	admin_plugins	locator_adm,config_adm,ifr_ad	sequence
🥏 IT_MgmtORB Ø iona_services	o2k.data.root	f:\e2a\var	string
COMet	o2k.domain.root	f:\e2a\etc	string
🚞 binding	admin_parser_name	admin_parser.tcl	string
🚞 plugins	IT_LocatorReplicas	iona_services.locator=corbaloc:i	sequence
irl_protocols in url_protocols	config.domain.name	configrep_domain	string
load_balancers	config.domain.type	cfr	string
i value_factories	config.domain.owner		string
🚞 initial_references	config.domain.secure	false	string
🕨 🔚 sample-domain	config.daemon.install	false	boolean
	export_config.orbacus	false	boolean
	IT_NameServiceReplicas	iona_services.naming=IOR:010	sequence
	IT_ConfigRepositoryReplicas	iona_services.config_rep=corba	sequence

Configuration variable settings

You can modify configuration variable settings in the **Configuration View** details pane. **For each configuration variable**, the **details pane provides the following text fields:**

• Name

Value

IDL Type

Modifying configuration variables

To modify configuration variable settings, perform the following steps:

Step	Action
1	Expand your selected domain in the navigation tree.
2	Navigate to the appropriate scope or namespace. The contained variables appear in the details pane.

Step	Action
3	Click the appropriate text field in the details pane. This is shown in Figure 36.
	or
	Click the IDL Type field to make a selection from the drop-down box.
4	Type your variable setting. Figure 36 shows setting a port number for the naming service.

Figure 36 Modifying a Configuration Variable



Creating Configuration Settings

You can create configuration settings using toolbar icons and the menu bar. This section explains how to create configuration scopes, namespaces, and variables. It includes the following:

- Loading up a domain
- Creating scopes
- Creating namespaces
- Creating variables

Note

You can create settings in a CFR domain only. You can not use this tool to create settings in a filebased domain. You should edit your configuration file instead.

Loading up a domain

Before you can create configuration settings, you must first load up your selected domain in the navigation tree.

To load up a domain, click the domain in the navigation tree. The domain icon in the navigation tree changes to a loaded domain, and the variables in the root configuration scope are displayed in the details pane, as shown in Figure 35 on page 52.

Creating scopes

To create a configuration scope in a domain, perform these steps:

Step	Action
1	Expand your selected domain in the navigation tree.
2	Navigate to the configuration scope or namespace in which you want to create the scope.
3	Click the Create a new scope button in the toolbar: 🥙
	Alternatively, you can select Edit>New Scope in the main menu.

Step	Action
4	Type your chosen new scope name in the Create a new scope dialog, as shown in Figure 38.
5	Press Enter.

Figure 37 Creating a Configuration Scope

Create a	new scope	×
3	new_scope_name] כ
	OK Cancel	

Creating namespaces

Step	Action
1	Expand your selected domain in the navigation tree.
2	Navigate to the configuration scope or namespace in which you want to create the namespace.
3	Click the Create a new namespace icon in the toolbar: Alternatively, you can select Edit>New Namespace in the main menu. Figure 38 shows the newly created namespace.
4	Click the new namespace name to edit it.
5	Type your chosen new namespace name.
6	Press Enter .

To create a configuration namespace, perform the following steps:

Figure 38 Creating a Configuration Namespace

▶ IONA Configuration Explorer 6.0				
<u>D</u> omain <u>E</u> dit <u>H</u> elp				
۵ 🖬 🍳				
Contents	Deta	ils		
 Domains configrep_domain IPAC_ORB IPAC_UTIL IT_MgmtORB Ona_services IT_oligins policies policies event_log configuration new_context_0 config_rep management comagement comagement conde_daemon COMet binding plugins url_protocols url_resolvers load_balancers 		Name	Value	IDL Type
Nonfiguration				

Creating variables

To create a configuration variable in a domain, perform the following steps:

Step	Action
1	Expand your selected domain in the navigation tree.
2	Navigate to the configuration scope or namespace in which you want to create the variable.
3	Click the Create a new variable icon in the toolbar:
	Alternatively, you can select Edit>New Variable in the main menu. Figure 39 shows a newly created variable in the root scope of the production domain.

Step	Action
4	Populate the new variable fields in the details pane with settings.
	Click the two text fields to type your settings. Click the IDL Type field to make a selection from the drop-down box.

Figure 39 Creating a Configuration Variable

2 🖻 🔢 🤍			
Contents	Details	1	1
 Domains configrep_domain IPAC_ORB IPAC_UTIL IT_MgmtORB IT_MgmtORB COMet binding plugins url_protocols url_resolvers load_balancers value_factories 	Name domain orb_plugins admin_plugins o2k.data.root new_variable_1 o2k.domain.root admin_parser_name IT_LocatorReplicas config.domain.name config.domain.type	Value itconfig://IOR:0100000024 local_log_stream,iiop_prof locator_adm,config_adm,if f\e2a\var new_variable_1 f\e2a\etc admin_parser.tcl iona_services.locator=corb configrep_domain cfr	sequence string string string string sequence string string
initial_references ©- <mark>न</mark> sample-domain	config.domain.owner config.domain.secure config.daemon.install	false false	string string boolean
	export_config.orbacus IT_NameServiceReplicas	false iona_services.naming=10	boolean sequence
	IT_ConfigRepositoryReplic	iona_services.config_rep=	sequence

Deleting Configuration Settings

This section explains how to delete configuration namespaces, and variables. It includes the following:

- Deleting scopes and namespaces
- Deleting variables

Note

You can delete settings in a CFR domain only. You can not use this tool to delete settings in a filebased domain. You should edit your configuration file instead.

The default configuration settings are suitable for most environments. For detailed information about configuration settings, see Finding Configuration Settings.

Deleting scopes and namespaces

To delete configuration scopes or namespaces in a domain, perform the following steps:

Step	Action
1	Expand your selected domain in the navigation tree.
2	Navigate to the appropriate configuration namespace.
3	Select Edit>Delete in the main menu. Alternatively, you can press the Delete key.

Note

Deleting a namespace deletes all the contained scopes or namespaces.

Deleting variables

Step	Action
1	Expand your selected domain in the navigation tree.
2	Navigate to the appropriate configuration scope or namespace.
3	Click a variable field in the details pane.
4	Select Edit>Delete in the main menu. In Figure 40 the variable created in Creating a Configuration Variable has been deleted.

To delete configuration variables in a domain, perform the following steps:

Figure 40 Deleting a Configuration Variable

🖉 📴 👪 🔍			
Contents	Details		
🖏 Domains	Name	Value	IDL Type
🛛 📋 configrep_domain	domain	itconfig://IOR:010000002400000	string
IPAC_ORB	orb_plugins	local_log_stream,iiop_profile,gi	sequence
🥥 IPAC_UTIL 🥥 IT_MgmtORB	admin_plugins	locator_adm,config_adm,ifr_ad	sequence
🥥 in_mgmiORB	02k.data.root	f:\e2a\var	string
COMet	o2k.domain.root	f:\e2a\etc	string
🚞 binding	admin_parser_name	admin_parser.tcl	string
plugins	IT_LocatorReplicas	iona_services.locator=corbaloc:i	sequence
in url_protocols in url_resolvers	config.domain.name	configrep_domain	string
load_balancers	config.domain.type	cfr	string
initial_references	config.domain.owner		string
	config.domain.secure	false	string
🛯 🔚 sample-domain	config.daemon.install	false	boolean
	export_config.orbacus	false	boolean
	IT_NameServiceReplicas	iona_services.naming=IOR:010	sequence
	IT_ConfigRepositoryReplicas	iona_services.config_rep=corba	sequence

Management Service Configuration

This section explains how the Orbix management service gets its configuration, and shows an example in the Orbix Configuration Explorer.

You can configure the Orbix management service by directly editing your configuration file. Configuration files are stored in the install-dir/etc/domains directory

Management service scope

The management service gets its configuration from the iona_services:management configuration scope in your configuration file.

If the configuration variables in the iona_services:management scope are not configured correctly, the management service starts up, and sends warnings to the event log and standard error. Depending on the particular variable, a default value is used, or the feature is not enabled (for example, if a persistent filename is not configured, persistent storage is not enabled).

Example configuration file

The following extract from a configuration file shows example configuration variables in the iona_services:management SCOPE:

```
management
{
    event_log:filters=["IT_MGMT_SVC=INFO_HI,WARN,ERR,FATAL"];
plugins:local_log_stream:filename =
    "install-dir/var/domain-name/logs/mgmt_svc.log";
    .
    .
    .
    .
    .
    .
};
```

This section explains how to use the iona_services:management variables to configure management service features.

Orbix Configuration Explorer example

Figure 41 shows management configuration variables in the Orbix Configuration Explorer.

For information about how to use the Orbix Configuration Explorer to manage configuration variables, see Managing Configuration Settings.

Figure 41 Orbix Configuration Explorer

Domain Edit Help				
Contents		Details		
locator		Name	Value	IDL Type
📕 🚽 🥏 otstm		ping_interval	10	string
event		idle_period	600	string
📄 🥏 🥏 management		persistent_filename	f:\orbix\var\my-domain\d	string
policies				
event_listener				
- initial_references				
event_processor				
event_barrier				
agent_container	-			
— 📄 severity_assigner				
web_server				
snmp_trap				
│				
- binding				
event_log				
event_history				
Ready				
Configuration				

Configuring the Event Log

This section explains how to enable the event log for management service events, and how to send the event log output to a file.

Configuring the event log filter

To enable event logging for the management service, you must set the required event severities for the IT_MGMT_SVC subsystem. You can specify these event severities using the event_log_filters configuration variable in the iona_services:management configuration scope.

The following example shows a recommended default setting in a configuration file:

```
event_log:filters="{IT_MGMT_SVC=INF0_HI+WARN+ERROR+FATAL}";
```

The following setting enables logging for all management service events:

```
event_log:filters = "{IT_MGMT_SVC=*}";
```

Sending the log output to a file

By default, Orbix logs event messages to a file. To change the location of this file, update the following variable in the iona_services:management configuration scope:

```
plugins:local_log_stream:filename =
"install-dir/var/domain-name/logs/mgmt_svc.log"
```

Configuring the local log stream

When running the management service, if the configured log file does not appear, you might need to add the local_log_stream plugin to the orb_plugins variable. For example:

```
orb_plugins = ["local_log_stream", "iiop_profile", "giop", "iiop", "ots"];
```

These configuration variables must be set correctly in order for the management service to write to the event log file.

Configuring Resource Agents

This section describes how to configure resource agent files and resource agent timeouts for the management service.

You must set all configuration variables for the management service in the management configuration scope.

Resource agents

Managed server applications register a resource agent reference with the management service. This enables a managed server to be made available for management. Resource agent references are stored in your file system.

A resource agent is an interface to a JMX instrumentation plugin in a managed server. A resource agent is loaded into a managed server to export server MBean information to the management service and management consoles. A resource agent is the sole entry point into a managed server.

Resource agents are registered with the management service, using a unique name, when they are loaded. Resource agents normally unregister when their server terminates; however, abnormal termination can result in references remaining in your system.

Configuring a resource agent file

You can use the following variable to specify the name of the persistent file in which resource agent references are stored:

```
agent_container:persistent_filename =
"install-dir/var/domain-name/mgmt/persistent/agents";
```

If an agents file is not specified (or if the file can not be created) the persistent storage is disabled. This means that a restarted management service does not know about the registered resource agents.

Configuring resource agent timeouts

You can use the following variable to specify the timeout in seconds to wait between repeatedly pinging all agents to verify that they are running:

```
agent_container:ping_interval = "10";
```

You can specify a timeout value of any number greater than **o** seconds. The default value is **1o** seconds.

Configuring Event Listeners

Client applications requesting events from the management service can register an event listener, so that all events are passed to those clients immediately. This section explains how to configure support for event listeners in the management service.

You must set all configuration variables for the management service in the iona_services:management configuration scope.

Configuring an event listener file

Use the following variable to specify the persistent file in which event listener references are stored:

```
event_processor:persistent_filename =
"install-dir/var/domain-name/mgmt/persistent/listeners";
```

If a listeners file is not specified (or if the file can not be created), the persistent storage is disabled. This means that a restarted management service does not know about the registered event listeners.

Configuring an event listener timeout

Use the following variable to specify the timeout in seconds to wait between repeatedly pinging all event listeners to verify that they are running:

```
event_processor:ping_interval = "10";
```

You can specify a timeout value of any number greater than **o** seconds. The default value is **1o** seconds.

Configuring Event History

This section explains how to configure an event history file, the event history memory capacity, and the interval at which event history is purged. You must set all configuration variable values for the management service in the management configuration scope.

Event history

Events received by the management service from managed applications are stored in the file system, so that they can be retrieved later.

You can specify the event history capacity to prevent the system from becoming overloaded. The recommended capacity is 1000 events. You can also specify an interval after which the event history file is purged. The default interval is 10 minutes.

Configuring an event history file

Use the following variable to specify the persistent file in which event history is stored:

```
event_history:persistent_filename = "install-dir/var/domain-name/mgmt/
persistent/events";
```

If an events file is not specified (or if the file can not be created), the persistent storage is disabled.

Configuring event history memory

Use the following variable to specify the number of events that are stored:

```
event_history:memory_capacity = "1000";
```

The default number of events is 1000. The maximum number of events is 4000. You must specify a positive value.

Configuring event history purges

Use the following variable to specify the interval at which the event history is purged:

```
event_history:trim_interval = "600";
```

The default is 600 seconds (10 minutes). You must specify a positive value.

Configuring Event Filters

Client applications requesting events from the management service use a named event filter to maintain their own event severity mapping and event threshold values. This section explains how to specify event severity files, and an event threshold file.

Configuring an event severity file

Use the following variable to specify where event severities are stored in the file system:

```
severity_assigner:persistent_filename = "install-dir/var/domain-name/mgmt/
persistent/severities";
```

The severities file is an internally used archive.

Configuring an event filter threshold file

Use the following variable to specify where event filter thresholds are stored in the file system:

```
event_barrier:persistent_filename = "install-dir/var/domain-name/mgmt/
persistent/threshold";
```

The threshold file is an internally used archive.

Configuring a default event severity file

You can also specify default event severity mapping using a default severity file. The event severities specified in this file apply to all new filters. The default event severity file is a pure text file, containing event name and event severity pairs, for example <code>com.iona.management.testevent 0</code>

Event severities

Valid event severities are represented by integers in the 0...3 range:

0	CRITICAL
1	ERROR
2	WARNING
3	INFO

Use the following variable to specify where the default event severity file is stored in your file system:

```
severity_assigner:default_filename = "install-dir\var\domain-
name\mgmt\persistent\default_severities.txt";
```

Configuring Event Processing

This section explains how to configure consolidated logging, an idle event period, and a logfile filter.

You must set all configuration variable values for the management service in the iona_services:management configuration scope.

Consolidated logging

Successive events with identical names and property values are treated as identical by a consolidated logging feature. This means that such follow-up events are eliminated and reported collectively at a later time (either after some delay, or before the next different event).

You should leave this consolidated event feature enabled, because it protects the system by reducing event numbers.

Enabling consolidated logging

Use the following variable to control consolidated logging:

```
event_listener:consolidated_logging = "true";
```

The default setting is true.

Configuring an idle event period

Idle event filters are removed and recreated internally in an identical state for further requests only. Use the following variable to specify the number of seconds an event filter is kept alive in memory:

```
event_processor:idle_period = "600";
```

Configuring the logfile filter

The event log contains a human-readable log of all the management events that have passed through the logfile filter (a reserved system filter). The logfile filter is used by the management service to generate tab-separated text files.

Use the following variable to specify where these event log text files are stored in your system:

event_log:filename_base = "install-dir/var/domain-name/mgmt/logs/events";

These filenames are appended with the a timestamp in the standard format .ddMMyyyy. For example: events.08102001

Configuring the Management Service Web Server

The Administrator Web Console serves as a web browser interface for HTTP-based access to the management service. This section shows how to configure the web server for this browser interface.

Configuring the web server

The web server's port number is specified by the web_server:port_number configuration variable in the liona_services:management scope. The default value is 53185. If this variable or port number is not found, the web server is disabled.

Orbix Configuration Explorer example

Figure 42 shows a configuration setting for the web server's port number in the Orbix Configuration Explorer.



Figure 42 Orbix Configuration Explorer Example

Enterprise Performance Logging

Rocket Software's performance logging plugins enable Orbix to integrate effectively with Enterprise Management Systems (EMS).

Introduction

Performance logging plugins enable Orbix to integrate effectively with *Enterprise Management Systems* (EMS), such as IBM Tivoli[™], HP OpenView[™], CA Unicenter[™], or BMC Patrol[™]. The performance logging plugins can also be used in isolation or as part of a bespoke solution.

Enterprise Management Systems enable system administrators and production operators to monitor enterprise-critical applications from a single management console. This enables them to quickly recognize the root cause of problems that may occur, and take remedial action (for example, if a machine is running out of disk space).

Performance logging

When performance logging is configured, you can see how each Orbix server is responding to load. The performance logging plugins log this data to file or syslog. Your EMS (for example, IBM Tivoli) can read the performance data from these logs, and use it to initiate appropriate actions, (for example, issue a restart to a server that has become unresponsive, or start a new replica for an overloaded cluster).

Example EMS integration

Figure 43 shows an overview of the Orbix Tivoli integration at work. In this example, a restart command is issued to an unresponsive server.

In Figure 43, the performance log files indicate a problem. The Orbix Tivoli Provider uses the log file interpreter to read the logs. The provider sees when a threshold is exceeded and fires an event. The event causes a task to be activated in the Tivoli Task Library. This task restarts the appropriate server.

This section explains how to manually configure the Orbix performance logging plugins. It also explains the format of the Orbix performance logging messages.

For details on how to integrate your EMS environment with Orbix, see the guide for your EMS.



Figure 43 Overview of an Orbix and IBM Tivoli Integration

Configuring Performance Logging

This section explains how to manually configure performance logging. This section includes the following:

- Performance logging plugins.
- Monitoring Orbix requests.
- Logging to a file or syslog.
- Monitoring clusters.
- Configuring a server ID.
- Configuring a client ID.
- Monitoring the Orbix work queue.
- Configuring performance logging with the GUI.

Note

You can also use the **Orbix Configuration** GUI (itconfigure command) to configure performance logging automatically. The manual configuration gives you more fine-grained control.

Performance logging plugins

The performance logging component consists of three plugins:

Table 6: Performance logging plugins

Plugin	Description
Response time logger	Monitors response times of requests as they pass through the Orbix binding chains. This can be used to collect response times for CORBA, RMI- IIOP or HTTP calls.
Request counter	Performs the same function for Artix as the Response time logger does for Orbix.
Response time collector	Periodically harvests data from the response time logger and request counter plugins and logs the results.
MBean monitor	Periodically harvests statistics associated with MBean attributes (for example, monitoring the length of the ORB work queue).

Monitoring Orbix requests

You can use performance logging to monitor both Orbix server and client requests.

Monitoring server requests

To monitor Orbix server requests, perform the following configuration steps:

1. Add it_response_time_logger to the servlet binding list for the server you wish to instrument. For example:

```
binding:servlet_binding_list= [
"it_response_time_logger + it_servlet_context + it_character_encoding
+ it_locale + it_naming_context + it_exception_mapping + it_http_sessions
+ it_web_security + it_servlet_filters + it_web_redirector +
it_web_app_activator "
];
```

2. Add it_response_time_logger to the server binding list for the server. For example:

```
binding:server_binding_list=[
"it_response_time_logger+it_naming_context+CSI+j2eecsi+OTS+it_security_role_mapping",
"it_response_time_logger+it_naming_context +
CSI+j2eecsi+it_security_role_mapping",
"it_response_time_logger+it_naming_context+it_security_role_mapping",
"it_response_time_logger+it_naming_context", "it_response_time_logger"
];
```

3. Add it_response_time_logger to the orb_plugins list for the server. For example:

```
orb_plugins=[
"it_servlet_binding_manager", "it_servlet_context",
"it_http_sessions", "it_servlet_filters", "http",
"it_servlet_dispatch", "it_exception_mapping", "it_naming_context",
"it_web_security", "it_web_app_activator",
"it_default_servlet_binding", "it_security_service", "it_character_encoding",
"it_locale", "it_classloader_servlet","it_classloader_mapping",
"it_web_redirector", "it_deployer",
"it_response_time_logger"
];
```

Monitoring client requests

To monitor Orbix client requests, add it_response_time_logger to the client binding list for the server. For example:

```
binding:client_binding_list = [
"it_response_time_logger+DemoOS+OTS+POA_Coloc","it_response_time_logger+DemoOS+F
"it_response_time_logger+OTS+POA_Coloc", "it_response_time_logger+POA_Coloc",
"it_response_time_logger+DemoOS+OTS+GIOP+IIOP",
"it_response_time_logger+OTS+GIOP+IIOP", "it_response_time_logger+GIOP+IIOP",
"it_response_time_logger"
];
```

Logging to a file or syslog

You can configure the collector plugin to log data either to a file or to syslog. The configuration settings for logging to a file depends on whether your application is written in C++ or Java:

C++ configuration

The following example configuration for a C++ application results in performance data being logged to /var/log/my_app/perf_logs/treasury_app.log every 90 seconds:

```
plugins:it_response_time_collector:period = "90";
plugins:it_response_time_collector:filename =
"/var/log/my_app/perf_logs/treasury_app.log";
```

If you do not specify the response time period, it defaults to 60 seconds.

Java configuration

Configuring the Java collector plugin is slightly different from the C++ collector) because the Java collector plugin makes use of Apache Log4J. Instead of setting plugins:it_response_time_collector:filename, you set the plugins:it_response_time_collector:log_properties to use Log4J, for example:

```
plugins:it_response_time_collector:log_properties = [
"appender.A1.type=RollingFile",
"appender.A1.name=A1",
"appender.A1.fileName=/var/log/my_app/perf_logs/treasury_app.log",
"appender.A1.filePattern=/var/log/my_app/perf_logs/treasury_app.log.%d{YYYY-
MM-dd}",
"appender.A1.layout.type=PatternLayout",
"appender.A1.layout.pattern=%d{ISO8601} %-80m %n",
"appender.A1.policies.time.type=TimeBasedTriggeringPolicy",
"appender.A1.policies.time.interval=1",
"appender.A1.policies.time.interval=2",
"appender.A1.strategy.type=DefaultRolloverStrategy",
"rootLogger.level=INFO",
"rootLogger.appenderRef.appender_ref.ref=A1"]
```

Logging to a syslog daemon

You can configure the collector to log to a syslog daemon or Windows event log, as follows:

```
plugins:it_response_time_collector:system_logging_enabled = "true";
plugins:it_response_time_collector:syslog_appID = "treasury";
```

The syslog_appid enables you to specify your application name that is prepended to all syslog messages. If you do not specify this, it defaults to iona.

Monitoring clusters

You can configure your EMS to monitor a cluster of servers. You can do this by configuring multiple servers to log to the same file. If the servers are running on different hosts, the log file location must be on an NFS mounted or shared directory.

Alternatively, you can use syslogd as a mechanism for monitoring a cluster. You can do this by choosing one syslogd to act as the central logging server for the cluster. For example, say you decide to use a host named teddy as your central log server. You must edit the /etc/syslog.conf file on each host that is running a server replica, and add a line such as the following:

```
# Substitute the name of your log server
user.info @teddy
```

Some syslog daemons will not accept log messages from other hosts by default. In this case, it may be necessary to restart the syslogd on teddy with a special flag to allow remote log messages.

You should consult the man pages on your system to determine if this is necessary and what flags to use.

Configuring a server ID

You can configure a server ID that will be reported in your log messages. This server ID is particularly useful in the case where the server is a replica that forms part of a cluster.

In a cluster, the server ID enables management tools to recognize log messages from different replica instances. You can configure a server ID as follows:

```
plugins:it_response_time_collector:server-id = "Locator-1";
```

This setting is optional; and if omitted, the server ID defaults to the ORB name of the server. In a cluster, each replica must have this value set to a unique value to enable sensible analysis of the generated performance logs.

Configuring a client ID

You can also configure a client ID that will be reported in your log messages. Specify this using the client-id configuration variable, for example:

```
plugins:it_response_time_collector:client-id = "my_client_app";
```

This setting enables management tools to recognize log messages from client applications. This setting is optional; and if omitted, it is assumed that a server is being monitored.

Monitoring the Orbix work queue

The it_mbean_monitoring plug-in enables you to periodically harvest statistics associated with MBean attributes. This plug-in can be used to monitor the work queue MBean associated with a particular ORB. Work queues are used to control the flow incoming requests.

To monitor an ORB work queue MBean, perform the following steps:

1. Add it_mbean_monitoring to the orb_plugins list of the ORB whose work queue you wish to monitor.

```
orb_plugins = ["local_log_stream", "iiop_profile", "giop", "iiop",
"it_mbean_monitoring"];
```

2. When it_mbean_monitoring is on your orb_plugins list, you can enable monitoring of the ORB work queue using the following variable:

plugins:it_mbean_monitoring:workqueue = "true";

3. The MBean attributes that are monitored by the plug-in are sampled periodically. The sampling interval is specified in milliseconds using the following variable:

plugins:it_mbean_monitoring:sampling_period = "100";

4. The response time collector plug-in is used to periodically log the MBean data. You must specify the following variables for the collector:

plugins:it_response_time_collector:period = "10";

C++ applications

plugins:it_response_time_collector:filename = "testing_mbeans.log";

Java applications

```
plugins:it_response_time_collector:log_properties = [
"appender.A1.type=RollingFile",
"appender.A1.name=A1",
"appender.A1.fileName=Z:\\art\\var\\filedomain\\logs\
\mbean_monitoring_perf.log",
"appender.A1.filePattern=Z:\\art\\var\\filedomain\\logs\"
\mbean_monitoring_perf.log.%d{YYYY-MM-dd}",
"appender.A1.layout.type=PatternLayout",
"appender.A1.layout.pattern=%d{IS08601} %-80m %n",
"appender.A1.policies.type=Policies",
"appender.A1.policies.time.type=TimeBasedTriggeringPolicy",
"appender.A1.policies.time.interval=1",
"appender.A1.policies.time.modulate=true",
"appender.A1.strategy.type=DefaultRolloverStrategy",
"rootLogger.level=INFO",
"rootLogger.appenderRef.appender_ref.ref=A1"]
```

For more information, see also MBean log message formats.

Configuring performance logging with the GUI

The **Orbix Configuration** GUI tool (itconfigure command) automatically generates performance logging configuration for the Orbix services. The generated server-id defaults to the following format:

domain-name_service-name_hostname (for example, mydomain_locator_myhost)

Logging Message Formats

This section describes the logging message formats used by Orbix and related products. It includes the following:

- Orbix log message format.
- Artix log message format.
- MBean log message formats.
- MBean log message formats.

Orbix log message format

Performance data is logged in a well-defined format. For Orbix applications, this format is as follows:

```
YYYY-MM-DD HH:MM:SS server=*serverID* [operation=*name*] count=*n* avg=*n* max=*n* min=*n* int=*n* oph=*n*
```

Argument	Description
server	The server ID of the process that is logging the message.
operation	The name of the operation for CORBA invocations or the URI for requests on servlets.
count	The number of operations of invoked (IIOP). or The number of times this operation or URI was logged during the last interval (HTTP).
avg	The average response time (milliseconds) for this operation or URI during the last interval.
max	The longest response time (milliseconds) for this operation or URI during the last interval.
min	The shortest response time (milliseconds) for this operation or URI during the last interval.
int	The number of milliseconds taken to gather the statistics in this log file.
oph	Operations per hour.

Table 7: Orbix log message format arguments

Artix log message format

The format for Artix log messages is as follows:

```
YYYY-MM-DD HH:MM:SS server=*serverID* [namespace=*nnn* service=*sss*
port=*ppp* operation=*name*] count=*n* avg=*n* max=*n* min=*n* int=*n*
oph=*n*
```

Table 8: Artix log message format arguments

Argument	Description
server	The server ID of the process that is logging the message.
namespace	An Artix namespace.
service	An Artix service.
port	An Artix port.

The combination of namespace, service and port above denote a unique Artix endpoint. The description for the remainder of the fields are the same as for Orbix messages.

MBean log message formats

The format for the mbean monitoring log message is as follows:

```
12004-09-23 15:24:17,093 monitored_object=*full-object-name-for-mbean*
object_alias=*user-friendly-name* count=*n* avg=*n* max=*n* min=*n*
period=*n*
```

Table 9: MBean log message format arguments

<pre>monitored_ob ject</pre>	The MBean being monitored (for example, DefaultDomain:type=AutoW orkqueue,orb=_it_orb_id_1,name=Workqueue_1).
object_alias	A user-friendly name for MBean being monitored (for example, test.man agement. logging_mbeans.ORBWorkQueue).
count	The number of times the MBean attribute has been sampled during this logging period.
avg	The average value for the attribute being monitored.

max	The maximum value for the attribute being monitored.
min	The minimum value for the attribute being monitored.
period	The sampling interval specified in milliseconds.

Simple life cycle message formats

The server also logs simple life cycle messages. All servers share the following common format.

YYYY-MM-DD HH:MM:SS server=*serverID* status=*current_status*

Table 10: Simple life cycle message format arguments

Argument	Description
server	The server ID of the process that is logging the message.
status	A text string describing the last known status of the server (for example, start ing_up , running , shutting_down).

SNMP integration

Events received from the Orbix management service are converted into SNMP management information. This information is sent to designated hosts as SNMP traps, which can be received by any SNMP managers listening on the hosts. In this way, Orbix enables SNMP managers to monitor Orbixbased systems.

Orbix supports SNMP version 1 and 2 traps only.

SNMP gateway

Orbix provides an SNMP gateway between the management service and SNMP managers. Figure 45 shows the steps in this process:

- 1. Orbix events received by the management service are passed on to the SNMP gateway.
- 2. The information extracted from the events are converted to SNMP traps using the MIB designed for Orbix applications.
- 3. The SNMP traps are then sent to a list of hosts on which SNMP managers are running.

Figure 45 Overview of the SNMP Gateway



This diagram gives a simplified view of this process. The SNMP manager on each host also uses the Orbix MIB file to translate the SNMP trap information into text names and values that it can understand.

SNMP gateway plugin

The SNMP gateway plugs into the management service, as shown in Figure 45. The SNMP gateway enables Orbix events to be sent from the management service to specific SNMP manager hosts as SNMP traps.

Configuring the SNMP Gateway

This section explains how to configure the Orbix SNMP gateway. It explains the following:

- Configuring the SNMP gateway plugin.
- Specifying SNMP managers.
- SNMP manager list format.
- Specifying SNMP management events.
- Specifying SNMP event severities.
- Specifying severities using the command line.
- Installing the Orbix MIB file.

Configuring the SNMP gateway plugin

To enable the management service to load the SNMP plugin, add the following variable in the liona_services:management:server scope:

```
ms_plugins = ["webconsole", "snmp"];
```

Specifying SNMP managers

You can specify the SNMP managers that you wish to access by setting the snmp_trap:managers_list
configuration variable in the iona_services:management scope. This variable specifies the list of all SNMP
managers to which you wish to send the SNMP trap.

For example:

```
snmp_trap:manager_list = ["boston:162:public:2",
"dublin:9998:public:1"];
```

This example list contains two entries, and specifies sending traps to two SNMP managers.

SNMP manager list format

The format of each entry in the SNMP trap manager list is as follows:

"hostname:port_number:community_name:SNMP_protocol_version"

The hostname specifies the host on which the SNMP manager is running.

The port_ number is the port that the SNMP manager uses to listen for traps.

The community_name specifies the SNMP community in which the SNMP managers are listening. An SNMP manager can listen in a number of *communities*, which are like user groups. In this example, the SNMP managers will only receive events if they are listening with the community name public. This is the default in most SNMP installations.

The SNMP_protocol_version can be set to either 1 or 2.

Specifying SNMP management events

You can specify which management events get sent to the SNMP gateway before they are sent on as traps to the SNMP managers.

The management service receives management events from various managed servers. It forwards these management events to a number of registered listeners using one or more event filters. These event filters assign a priority to each event and forward or discard the events based on priority.

Using this mechanism, you can control which events are sent to the subscribers registered with a particular filter. The SNMP Gateway uses an event filter called SNMPFilter.

Example SNMP management events

An example application permits management events all beginning with the following prefix:

com.bigcompany.myapp

An administrator wishes to pass all of these events to the SNMP gateway but block all others. This means changing the default severity assignments. Management events are assigned a severity in the range 0 (Critical) to 3 (Information).

For more information about management events and filters, see Managing Events in the Web Console.

Specifying SNMP event severities

To specify event severities for the example management event, you must to perform the following steps:

- 1. Ensure that the default severity for the filter is set to 3 (Information).
- 2. Set the severity of all events whose names begin with the string com.bigcompany.myapp to 2 (Warning).
- Set the filter's threshold to 3. This means that the filter will permit all events with severity less than
 In this case, only events whose names begin with the string com.bigcompany.myapp will be sent to the SNMP Gateway.

Specifying severities using the command line

You can specify event severities for the example management events using a simple command-line tool as follows:

Step	Action
1	Set the environment for your domain, and ensure that all services including the management service are running, and configured to load the SNMP gateway plugin.
2	Start the command line tool as follows: java itiadmin.command -ORBdomain_name mydomain You can get help at any time by typing help.
3	Check the default severity for the SNMP gateway filter. itiadmin.command> default_severity show -filter SNMPFilter 3
4	Assign a severity of 2 to any events whose names begin with com.bigcompany.myapp: itiadmin.command> severity modify com.bigcompany.myapp 2 - filter SNMPFilter

Step	Action
5	Modify the threshold to pass only events whose severities are less than 3 (that is, permit only Warning=2, Error=1 or Critical=0 events).
	<pre>itiadmin.command> threshold modify 3 -filter SNMPFilter</pre>

Installing the Orbix MIB file

A Management Information Base (MIB) file is a database of objects that can be managed using SNMP. Orbix provides the iona_admin_mib.txt file, which describes the MIB for Orbix. This is file available in the following directory:

install-dir /asp/ version /doc/admin/

You should install the iona_admin_mib.txt file using your chosen third party management console (for example, HP OpenView). For information on how to import a MIB file, please consult the documentation for your chosen third-party console.

Note

SNMP is an unreliable protocol. If you are generating management events that are intended for an SNMP-based management console, you should continue to emit the event periodically until the cause of the error or event has been acknowledged or reset.

Glossary

Administration

All aspects of installing, configuring, deploying, monitoring, and managing a system.

Application Server

A software platform that provides the services and infrastructure required to develop and deploy middle-tier applications. Middletier applications perform the business logic necessary to provide web clients with access to enterprise information systems. In a multi-tier architecture, an application server sits beside a web server or between a web server and enterprise information systems. Application servers provide the middleware for enterprise systems.

CORBA

Common Object Request Broker Architecture. An open standard that enables objects to communicate with one another regardless of what programming language they are written in, or what operating system they run on.

Configuration

A specific arrangement of system elements and settings.

Controlling

The process of modifying the behavior of running software components, without stopping them.

Details Pane

The display pane on the right hand side of the Administrator Web Console user interface.

Deployment

The process of distributing a configuration or system element into an environment.

Domain

An abstract grouping of managed server processes and hosts within a physical location. Processes within a domain share the same configuration and distributed application infrastructure. A domain is equivalent to an Orbix configuration domain.

EJB

Enterprise Java Beans. Oracle's architecture for the development and deployment of reusable, object-oriented, middle-tier components. EJBs can be either session beans or entity beans. EJB enables the implementation of a multi-tier, distributed object architecture. See http://www.oracle.com/technetwork/java/index.html/

Event

An occurrence of interest, which is emitted from a managed entity.

Host

Generic term used to describe a computer, which runs parts of a distributed application.

Installation

The placement of software on a computer. Installation does not include Configuration unless a default configuration is supplied.

Instrumentation

Code instructions that monitor specific components in a system (for example, instructions that output logging information on screen.) When an application contains instrumentation code, it can be managed using a management tool such as Administrator.

Invocation

A request issued on an already active software component.

J2EE

Java 2 Enterprise Edition. An environment for developing and deploying enterprise applications. The J2EE platform consists of services, application programming interfaces (APIs), and protocols that provide the functionality for developing multi-tiered, Web-based applications.

JRE

Java Runtime Environment. A subset of the Java Development Kit required to run Java programs. The JRE consists of the Java Virtual Machine, the Java platform core classes and supporting files. It does not include the compiler or debugger.

JMX

Java Management Extensions. Sun's standard for distributed management solutions. JMX provides tools for building distributed, Web-based solutions for managing devices, applications and service-driven networks.

Managed Application

An abstract description of a distributed application, which does not rely on the physical layout of its components.

Managed Entity

A generic manageable component. Managed entities include managed domains, servers, containers, modules, and beans.

Managed Server

A set of replicated managed processes. A managed process is a physical process which contains an ORB and which has loaded the management plugin. The managed server can be an EJB application server, CORBA server, or any other instrumented server that can be managed by Administrator.

Managed Process.

A physical process which contains an ORB and which has loaded the management plugin.

Management

To direct or control the use of a system or component. Sometimes used in a more general way meaning the same as Administration.

MBean

A JMX term used to describe a generic manageable object.

Monitoring

Observing characteristics of running instances of software components. Monitoring does not change a system.

Navigation Trail

A linear list of managed servers on top of Details View, which shows the path taken to the currently displayed managed entity.

Navigation Tree

The tree on the left hand side of the Administrator Web Console and Orbix Configuration Explorer.

ORB

CORBA Object Request Broker. This is the key component in the CORBA architecture model. It acts as the middleware between clients and servers.

Process MBean

The is the first-level MBean that is exposed for management of an application. It is the starting point for navigation through an application in the Administrator Web Console

Runtime Administration, Runtime Management

Encompasses the running, monitoring, controlling and stopping of software components.

SNMP

Simple Network Management Protocol. The Internet standard protocol developed to manage nodes on an IP network. It can be used to manage and monitor all sorts of devices (for example, computers, routers, and hubs)

Starting

The process of activating an instance of a deployed software component.

Stopping

The process of deactivating a running instance of a software component.

Web Services

Web services are XML-based information exchange systems that use the Internet for direct application-to-application interaction. These systems can include programs, objects, messages, or documents.

Web Services Container

A Web services container provides an environment for deploying and running Web services. A Web services container is typically deployed and runs in an application server.

XML

Extensible Markup Language. XML is a simpler but restricted form of Standard General Markup Language (SGML). The markup describes the meaning of the text. XML enables the separation of content from data. XML was created so that richly structured documents could be used over the web. See http://www.w3.org/XML/

Notices

Copyright

© 1996-2025 Rocket Software, Inc. or its affiliates. All Rights Reserved.

Trademarks

Rocket is a registered trademark of Rocket Software, Inc. For a list of Rocket registered trademarks go to: www.rocketsoftware.com/about/legal. All other products or services mentioned in this document may be covered by the trademarks, service marks, or product names of their respective owners.

Examples

This information might contain examples of data and reports. The examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

License agreement

This software and the associated documentation are proprietary and confidentical to Rocket Software, Inc. or its affiliates, are furnished under license, and may be used and copied only in accordance with the terms of such license.

Note: This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when exporting this product.

Corporate information

Rocket Software, Inc. develops enterprise infrastructure products in four key areas: storage, networks, and compliance; database servers and tools; business information and analytics; and application development, integration, and modernization.

Website: www.rocketsoftware.com

Contacting Technical Support

The Rocket Community is the primary method of obtaining support. If you have current support and maintenance agreements with Rocket Software, you can access the Rocket Community and report a problem, download an update, or read answers to FAQs. To log in to the Rocket Community or to request a Rocket Community account, go to www.rocketsoftware.com/support. In addition to using the Rocket Community to obtain support, you can use one of the telephone numbers that are listed above or send an email to support@rocketsoftware.com.

Rocket Global Headquarters 77 4th Avenue, Suite 100 Waltham, MA 02451-1468 USA

Country and Toll-free telephone number

To contact Rocket Software by telephone for any reason, including obtaining pre-sales information and technical support, use one of the following telephone numbers.

- United States: 1-855-577-4323
- Australia: 1-800-823-405
- Belgium: 0800-266-65
- Canada: 1-855-577-4323
- China: 400-120-9242
- France: 08-05-08-05-62
- Germany: 0800-180-0882
- Italy: 800-878-295
- Japan: 0800-170-5464
- Netherlands: 0-800-022-2961
- New Zealand: 0800-003210
- South Africa: 0-800-980-818
- United Kingdom: 0800-520-0439