

IBM Intelligent Operations Center



# IBM Intelligent Operations Center Product Documentation

*Version 1 Release 0*



IBM Intelligent Operations Center



# IBM Intelligent Operations Center Product Documentation

*Version 1 Release 0*

**Note**

Before using this information and the product it supports, read the information in "Notices" on page 147.

This edition applies to IBM Intelligent Operations Center version 1, release 0, modification 0. This edition applies to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2011, 2012.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# Contents

## Figures . . . . . v

## Chapter 1. Solution overview. . . . . 1

Intended audience . . . . .	1
Features . . . . .	2
Users and benefits . . . . .	2
Components . . . . .	3
Event management . . . . .	5
What's new in the fix pack? . . . . .	6

## Chapter 2. Installing and configuring . . . 9

Preparing for installation . . . . .	9
System configuration . . . . .	9
Hardware requirements . . . . .	12
Software requirements . . . . .	14
Media packaging . . . . .	15
Installing the solution . . . . .	15
Preparing the servers . . . . .	16
Copying files required to install and deploy the solution . . . . .	18
Extracting installation files and installing dependencies . . . . .	18
Checking installation prerequisites . . . . .	19
Deploying the solution . . . . .	20
Deploying the package from a command line . . . . .	22
Running specific deployment tasks . . . . .	23
Installing Tivoli Service Request Manager . . . . .	23
Installing tools provided with the solution . . . . .	23
Post-installation configuration . . . . .	24
Setting the WebSphere Portal session timeout value . . . . .	24
Setting the Tivoli Access Manager WebSEAL session cache settings timeout value . . . . .	25
Configuring single sign-on . . . . .	25
Creating a WebSphere Application Server Network Deployment junction . . . . .	30
Configuring WebSphere Application Server Network Deployment for LTPA single sign-on . . . . .	31
Enabling login redirection . . . . .	32
Configuring the REST Services Gateway port and protocol . . . . .	32
Deleting sample users . . . . .	33
Verifying the solution installation . . . . .	33
Verifying the publishing of CAP events . . . . .	35
Installing and configuring the fix pack . . . . .	35
Preparing to install the fix pack . . . . .	35
Installing the fix pack . . . . .	41
Restarting a failed installation for the fix pack . . . . .	42
Post-installation configuration . . . . .	44

## Chapter 3. Securing the solution . . . . . 47

User roles and access . . . . .	48
Sample users . . . . .	49
User role groups and authorization permissions . . . . .	49
User category groups and data permissions . . . . .	51

Adding a user or group . . . . .	52
Viewing or modifying group membership . . . . .	53
Viewing or editing a user profile . . . . .	54
Deleting a user or group . . . . .	55
Security . . . . .	56
Managing a Tivoli Access Manager WebSEAL junction ACL . . . . .	56
Managing a Tivoli Access Manager WebSEAL junction ACL using the command line . . . . .	57
Managing a Tivoli Access Manager WebSEAL junction ACL using the Tivoli Access Manager WebSEAL Web Portal Manager . . . . .	57
Importing users and groups . . . . .	58

## Chapter 4. Integrating the solution. . . . . 59

Examples of systems that can be integrated. . . . .	59
Integration points and protocols . . . . .	59
Events and KPIs . . . . .	59
Integrating with the Common Alerting Protocol . . . . .	61
Integrating with other protocols . . . . .	69
Publishing CAP messages . . . . .	69
Sample Publisher . . . . .	69
Customizing KPIs . . . . .	72
Monitor models and KPIs . . . . .	73
Monitoring context instances . . . . .	74
Modeling KPIs . . . . .	74
Nested KPIs . . . . .	77
Defining KPI parent/child relationships . . . . .	78
KPI event communication between the IBM WebSphere Business Monitor and the IBM Intelligent Operations Center . . . . .	78
Deploying monitor models . . . . .	81
KPI display values . . . . .	82
Caching KPIs . . . . .	83
Sample KPIs . . . . .	83
Creating reports . . . . .	85

## Chapter 5. Customizing the solution . . . 87

Customizing the user interface . . . . .	87
Localizing the user interface . . . . .	87
List of portlets . . . . .	87
Customizing the page layout . . . . .	89
Configuring the map . . . . .	89
Specifying system-wide configuration data . . . . .	91
Updating the SYSPROP table . . . . .	93
Creating KPIs for use with the IBM Intelligent Operations Center . . . . .	93
Configuring IBM Cognos Business Intelligence to create reports in IBM Intelligent Operations Center . . . . .	94
Setting up an IBM Cognos Business Intelligence data source . . . . .	94
Importing the IBM Intelligent Operations Center analytics data model into IBM Cognos Business Intelligence . . . . .	95

## Chapter 6. Managing the solution . . . 97

Intelligent Operations Center - About . . . . .	97
Controlling components with <b>IOControl</b> . . . . .	97
Getting help for the <b>IOControl</b> command . . . . .	97
Starting components . . . . .	98
Starting the Tivoli Netcool/OMNIBus probe . . . . .	99
Stopping components . . . . .	99
Querying the status of components . . . . .	99
Fix pack server monitoring . . . . .	100
Starting and stopping server monitoring . . . . .	100
Managing the heartbeat service . . . . .	101
Maintaining the solution . . . . .	102
Tuning performance . . . . .	102
Managing log files. . . . .	102
Backing up data . . . . .	103
Maintenance tips . . . . .	105

## Chapter 7. Using the solution interface . . . . . 107

Logging on . . . . .	107
Logging off . . . . .	107
Viewing or editing your user profile. . . . .	108
Executive view . . . . .	108
Status . . . . .	109
Key Performance Indicator Drill Down . . . . .	110
Coordinator - Alerts . . . . .	111
Sametime Contacts . . . . .	113
Operations view . . . . .	113
Map . . . . .	114
Using the map controls . . . . .	115
Adding an event . . . . .	115
Configuring the map . . . . .	117
Events. . . . .	117
Managing existing events . . . . .	118
Adding an event . . . . .	119
Coordinator - Alerts . . . . .	119
Sametime Contacts . . . . .	121

## Chapter 8. Troubleshooting and support . . . . . 123

Techniques for troubleshooting problems . . . . .	123
Log files . . . . .	125
Installation management server log files . . . . .	125
Portal server log files. . . . .	125
Application and integration server log files . . . . .	126
Analytic server log files . . . . .	127
Event and management server log files. . . . .	128
Summary of systems and log file locations . . . . .	130
IBM Intelligent Operations Center Messages . . . . .	131
CHK: Installation prerequisite checking messages . . . . .	132
Searching knowledge bases. . . . .	135
Getting fixes from Fix Central . . . . .	136
Contacting IBM Support. . . . .	136
Exchanging information with IBM . . . . .	137
Sending information to IBM Support . . . . .	138
Receiving information from IBM Support . . . . .	138
Installing and using IBM Support Assistant Lite . . . . .	139
Subscribing to support updates . . . . .	139
Troubleshooting tips . . . . .	141
Restarting a failed installation for the fix pack . . . . .	142

## Chapter 9. References . . . . . 145

PDF library . . . . .	145
Additional information . . . . .	145
Copyright notice and trademarks. . . . .	146
Copyright notice . . . . .	146
Trademarks . . . . .	146

## Notices . . . . . 147

Trademarks . . . . .	148
----------------------	-----

## Index . . . . . 151

---

## Figures





---

## Chapter 1. Solution overview

Many organizations and endeavors require efficient operational supervision and coordination. All have in common the need for the right information to be brought together so that the right people can make fast, accurate decisions and track the effect of those decisions. The IBM® Intelligent Operations Center is a software solution designed to facilitate effective supervision and coordination of operations.

Authorities face common challenges in their core systems and in making improvements to systems that are interconnected. Authorities that are forward-looking want to use the improvements in efficiency and effectiveness of smarter core systems. They adopt new ways of thinking about and using these systems. The application of advanced information technology can help authorities better understand, predict, and intelligently respond to patterns of behavior and events.

For example, IBM defines an intelligent city in terms of the improvements in quality of life and economic well-being that are achieved through applying information technologies (IT) to plan, design, build, and operate the city infrastructure. An intelligent city is not primarily about "the latest technology." It is about finding ways to use technology to make the most effective use of the existing resources, to improve the life of the citizens of the city.

The IBM Intelligent Operations Center uses the power of the real-world data generated by computer systems by:

- Collecting and managing the right data
- Integrating and analyzing that data
- Facilitating easy and timely access to information
- Adjusting systems to achieve results based on the insights gained

The benefits of this solution are to:

- Optimize planned and unplanned operations using a holistic reporting and monitoring approach
- Build convergence of domains in an organization by facilitating communication and collaboration
- Improve quality of service and reduce expense by coordinating events

An operation can be divided into individual domains, which generally match with the organization structure and the expertise of the people involved. In a city, the expertise is held in departments, for example, in transportation, water, and public safety.

As the complexity of operations in a domain increases, a more customized solution is required. The IBM Intelligent Operations Center has a number of different integration points where customization can take place. These integration points and the infrastructure included give IBM Business Partners, service providers, and customers the flexibility to build a broad and powerful solution.

---

### Intended audience

This information center is intended for people who are using, installing, administering, and maintaining the IBM Intelligent Operations Center. It also contains implementation documentation for customizing the solution and integrating the external underlying systems that IBM Intelligent Operations Center requires.

This information center assumes that users have prior knowledge of or proficiency in using the component products included in this solution. Training for these component products is outside the scope of this information center. If you require training for these products, ask your systems integrator or IBM representative where you can obtain information about base component training opportunities.

You can find links to the component product documentation in the “Additional information” on page 145 section.

---

## Features

The IBM Intelligent Operations Center provides measuring, monitoring, and modeling facilities that integrate underlying systems into one solution to improve operational efficiency, planning, and coordination.

The IBM Intelligent Operations Center is a solution within the IBM Smarter Cities® Software Solutions product family. IBM Intelligent Operations Center can be installed on existing hardware (on premise) or it can be deployed in the cloud. IBM Intelligent Operations Center can be installed by itself, or you can install it with other solutions from the IBM Smarter Cities Software Solutions product family.

The IBM Intelligent Operations Center is a GUI-based solution with role-based access to events for an organization and underlying domains. It has event management, integrated mapping, and collaboration capabilities. It also has key performance indicator (KPI) reporting and business rules capability for improved effectiveness. This functionality provides authorities with the ability to integrate domains for improved cooperation and decision-making.

### Event and incident management

IBM Intelligent Operations Center provides an event reporting and tracking mechanism to enable identification and understanding across underlying domains. You can manage predicted events, planned events, and current events as they evolve. For example, replacing pipes that run under a road is a planned event or work order involving water and traffic. Inclement weather arriving in the next 24 hours is a predicted event. A traffic jam is a current event affected by both roadworks and weather.

An integrated geographic information system (GIS) maps events visually, enabling you to gauge the impact of events through interactive mapping and scenario analysis.

### Status reporting and monitoring

IBM Intelligent Operations Center provides a tool for creating and displaying KPIs. The KPIs can be updated as underlying data changes. You can use this tool to:

- Summarize executive-level status for a single domain or across domains
- Highlight issues and identify problems
- Investigate further by drilling down into the KPI details

### Instant notification and messaging

IBM Intelligent Operations Center provides a workspace where you can maintain alerts for matters that need attention. You can use this workspace to monitor news and events, especially when other portlets that announce news are not in view.

IBM Lotus® Sametime® provides an integrated collaboration and communication tool that you can use for instant messages where and when it is needed.

---

## Users and benefits

The IBM Intelligent Operations Center has been designed for personnel involved with operational control in organizations, government departments or local authorities: executives, supervisors, and operators.

The following table describes the users and benefits associated with using IBM Intelligent Operations Center.

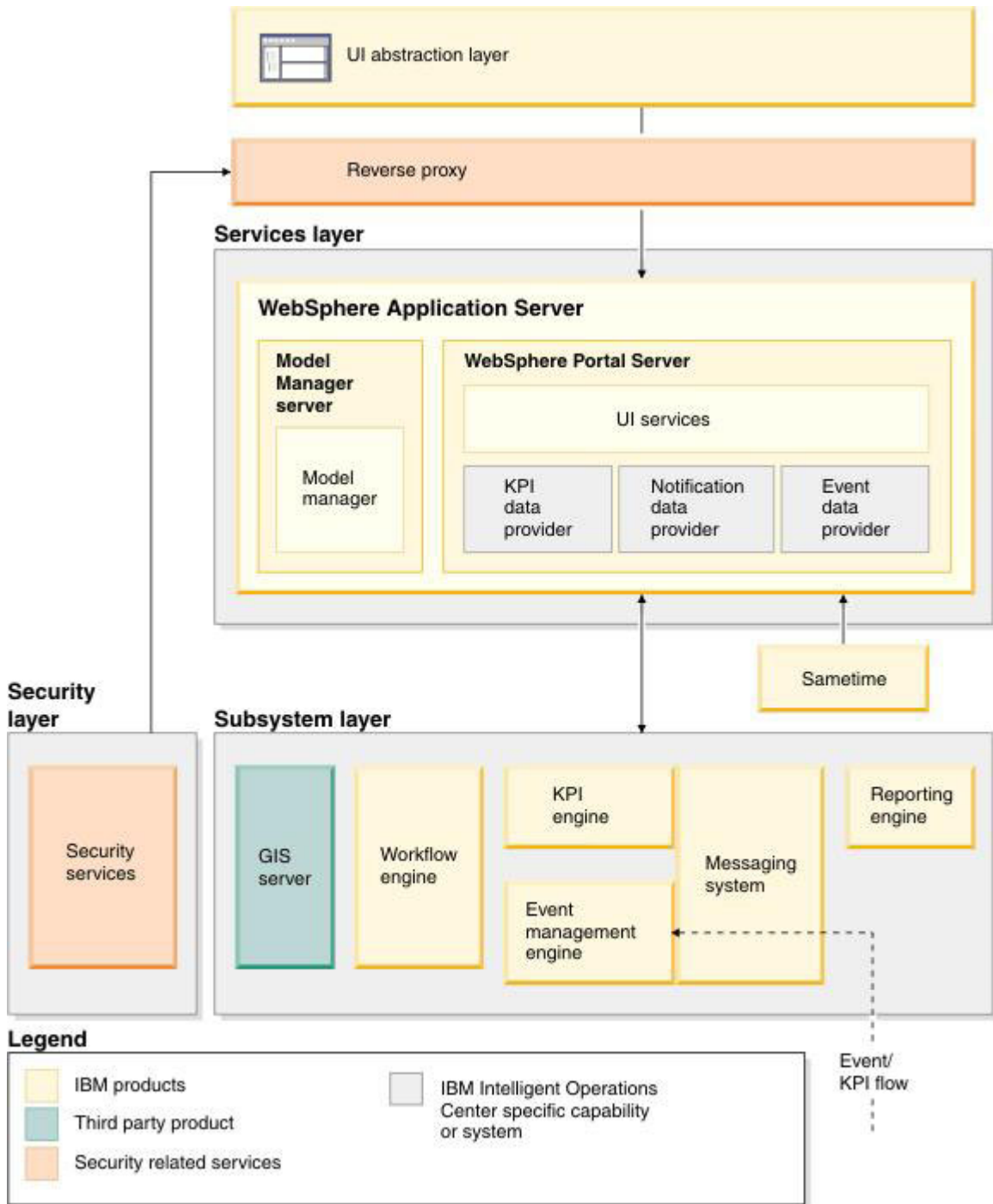
Table 1. IBM Intelligent Operations Center users and benefits

If you are a...	This software can help you...
Executive	<ul style="list-style-type: none"> <li>• Gain an executive level summary of events and incidents through maps, dashboards, and alerts</li> <li>• Determine measures of organizational success with key performance indicators (KPIs)</li> <li>• Identify and track issues using reports</li> <li>• Direct priorities and implementation of policy using data provided</li> </ul>
Supervisor	<ul style="list-style-type: none"> <li>• Identify and act on conflicts and issues shown on maps, dashboards, and alerts</li> <li>• Manage events by adding new events, editing existing events, canceling events, and escalating events to incidents</li> <li>• Monitor the KPIs that have been set up</li> <li>• Communicate quickly and easily on matters of importance</li> </ul>
Operator	<ul style="list-style-type: none"> <li>• Monitor status, create and edit events and incidents to be shown in lists</li> <li>• Notify appropriate manager or executives and issue alerts</li> <li>• Communicate quickly and easily in emergencies and other situations requiring a response</li> </ul>
User administrator	<ul style="list-style-type: none"> <li>• Add new users and assign them to groups</li> <li>• Ensure security through role-based authorization groups with appropriate permissions</li> <li>• Set up permissions appropriate to areas of expertise and data required</li> </ul>

## Components

At a high level the structure of the IBM Intelligent Operations Center can be divided into major components and subsystems.

The following diagram shows a high-level view of the main components of the IBM Intelligent Operations Center.



## UI abstraction layer

The IBM Intelligent Operations Center provides web-based, one-stop portals to event information, overall status, and details. The user interface (UI) presents customized information in various pre-configured views in common formats. All information is displayed through easy-to-use dashboards.

## Security layer

All access to information is controlled by the security layer through organizational roles and data categories. This control prevents unauthorized access while enabling easy management of entitlements.

## Services layer

The services layer uses common widgets and a common UI services framework to receive event data and pass it through event management to the message system. IBM Intelligent Operations Center data providers extend the UI services. Because of the wide variety of data coming from underlying operational systems, data is normalized according to a standard semantic reference model, which provides a common dictionary for mapping relationships. This model facilitates effect analysis and response to events without the need for multiple translations of information. Model manager provides access to KPI and hierarchy information of underlying domains. Advanced analytics can be performed on data, identifying optimizations and predictions that can help guide decision-making and governance.

## Subsystem layer

The solution provides a mediation layer to facilitate the information exchange between the solution and operational systems of underlying domains. Data from various configurable sources can be provided through gateways into a subsystem layer, which can generate alerts, KPIs and events. This integration layer enables the two-way communication of messages in various formats, using open standards where possible. By using industry standard tools to perform the transformation from sources to the reference semantic model, the underlying operational systems do not need to be changed. Emergency and other response systems can be connected to the IBM Intelligent Operations Center for appropriate workflows.

The structure of the IBM Intelligent Operations Center supports the following:

- A central point for understanding the state of operations, managing events and incidents, and connecting domains under operations center control
- Integration to a geographic information system (GIS) for mapping events and incidents spatially and visually
- Creation and display of key performance indicators (KPIs), which are updated as data changes through connections to underlying domain systems
- Alerts coming in from the field, including those requiring emergency or standard responses
- Collaboration capabilities, through instant messaging with IBM Lotus Sametime
- A role-based security model

---

## Event management

The IBM Intelligent Operations Center solution focuses on the integration and optimization of information within and across multiple domains in a central operations hub, in real-time and over long periods. Event management enables an operations center to assimilate data from multiple systems to constantly predict and react to significant events and trends.

Events are self-contained data items containing basic but complete information that recipients can respond to. Events are placed in queues by the IBM Intelligent Operations Center and processed by the event management engine.

Events come into the IBM Intelligent Operations Center in different forms based on the nature of the operations center. Some examples of the forms of event are triggers, thresholds, complex events, and manually-generated events.

Triggers are events generated by something happening and usually require an action to be taken by the recipient. Examples of triggers are:

- Fire or smoke alarms going off
- Information technology systems going down
- Intrusion detectors tripped
- Natural events picked up by sensors, such as earth tremors

The IBM Intelligent Operations Center can receive information on such events from external systems and convert it into alerts for recipients. In general, it is likely that lower level indicators would be summarized and only passed to the IBM Intelligent Operations Center if they merited wider attention. For example, all fires may not be reported as events. However, a fire involving multiple divisions of the fire service and environmental protection expertise, due to hazardous material, would merit reporting to the operations center.

Threshold events help you determine when the measurements obtained from a sensor or other source have moved outside the normal range. Basic threshold events are comparisons that compare two or more measures and report a trend. More sophisticated threshold events can compare measures against a threshold created by historical information. Examples of threshold events are:

- Over and under temperature alarms
- High and low water levels
- Air quality and water purity breaching environmental standards
- Excessive power consumption

The IBM Intelligent Operations Center can manage such events in the form of key performance indicators (KPIs).

Complex events bring together information from multiple systems to determine if a group of related events should be reported. For example, the toll road authority receives a trigger event from its monitoring system that indicates that the computer link for credit card authorization is down, followed shortly by a threshold event from the financial system warning that they are close to their credit limit for unauthorized payments. The combination of these two issues is much more serious than either in isolation, so a complex event is generated to raise awareness and coordinate a resolution.

Events that are entered manually are especially important to cities. Some of these are observed incidents, such as crimes and traffic accidents. Other examples of events entered manually are those generated from emergency calls from citizens, from reports made by city officials, or from management systems that report on city status. The most common types of event entered manually are:

- Severe weather warnings
- Crime reports
- Fires
- Road traffic incidents – accidents, congestion, unusual loads
- Upcoming events – rock concerts, road races, parades

Complex event processing allows a city to identify exceptions to city systems easily, occasionally to identify trends from unrelated data, and to predict future issues.

---

## What's new in the fix pack?

### Fix Pack 1

The IBM Intelligent Operations Center 1.0 Fix Pack 1 delivers stability improvements, upgrades to components, and system-monitoring infrastructure.

### Installation prerequisite check

There is a prerequisite check incorporated in the installation script for the fix pack. When you run the command to install the fix pack, prerequisite checking is performed automatically. For more details on how this check operates when installing the fix pack, see the related task linked at the end of the topic.

## Upgrades

The fix pack provides the following upgrades to components included in the IBM Intelligent Operations Center 1.0:

- IBM Integrated Information Core model manager from version 1.4 to 1.4.0.1
- WebSphere® Portal from version 7.0 to 7.0.0.2
- WebSphere Application Server from version 7.0.0.13 to 7.0.0.19
- Tivoli® Directory Server from version 6.2.0.1 to 6.2.0.3

As part of the middleware upgrade provided, Tivoli Service Request Manager® Version 7.2.1 is installed automatically with the fix pack.

## Single sign-on

Single sign-on is configured for IBM Cognos® Business Intelligence between the reporting function of the analytic server and the portal server. This configuration enables access to the reporting function through the access server via a Tivoli Access Manager WebSEAL junction. Single sign-on is also configured for Tivoli Service Request Manager. This configuration enables access to the IBM Maximo UI through the access server via a Tivoli Access Manager WebSEAL junction.

## WebSphere Application Server profile for IBM ILOG® CPLEX® Optimization Studio

The fix pack creates a WebSphere Application Server profile for deploying and hosting IBM ILOG CPLEX Optimization Studio applications.

## Additions to the `IOControl` command

When controlling servers with the `IOControl` command, there are three new targets for the `IOControl` script:

- `db24tsrm-IBM: DB2® Enterprise Server Edition for Tivoli Service Request Manager`
- `cplex-IBM: WebSphere Application Server for IBM ILOG CPLEX Optimization Studio`
- `tsrm-IBM: Tivoli Service Request Manager`

For more details on the `IOControl` command, see the related concept linked at the end of the topic.

## Monitoring agents

The following monitoring agents are installed by default:

- Tivoli Composite Application Manager for IBM HTTP Server
- Tivoli Composite Application Manager for Lotus Domino®
- Tivoli Composite Application Manager for IBM Lotus Sametime
- Tivoli Composite Application Manager for WebSphere Message Broker
- Tivoli Composite Application Manager for WebSphere MQ

In addition, the Tivoli Composite Application Manager monitoring agent for WebSphere MQ is configured by default during the installation. For more details on the fix pack server monitoring, see the related task linked at the end of the topic.

## Heartbeat service

The fix pack provides a heartbeat service to monitor the status and health and to perform automatic fault-recovery of middleware components. The service operates on all the middleware components in the IBM Intelligent Operations Center 1.0 Fix Pack 1 system configuration with the following exceptions:

- Access server: Tivoli Access Manager WebSEAL
- Analytic server: IBM ILOG CPLEX Optimization Studio
- Event and management server:
  - Tivoli Directory Server 6.2.0.3
  - Tivoli Directory Integrator 7.1
  - Tivoli Access Manager 6.1
  - Tivoli Identity Manager 5.1.0.0
  - IBM Tivoli Monitoring 6.2.2.1
  - Tivoli Composite Application Manager 6.2.4
  - WebSphere Application Server 6.0.0.23

For details on the system configuration, see the related concept linked at the end of the topic. For more details of the heartbeat service, see the related task linked at the end of the topic.

**Related concepts:**

“Controlling components with **IOControl**” on page 97

You can control or query the status of the IBM Intelligent Operations Center components by using the **IOControl** command.

“System configuration” on page 9

The IBM Intelligent Operations Center installs and configures an environment with production servers and one server used during the installation process.

**Related tasks:**

“Installing the fix pack” on page 41

Use the command line to install the IBM Intelligent Operations Center 1.0 Fix Pack 1.

“Fix pack server monitoring” on page 100

View the data collected by the Tivoli Enterprise Monitoring Agent.

“Managing the heartbeat service” on page 101

The heartbeat service provided with the IBM Intelligent Operations Center 1.0 Fix Pack 1 restarts middleware components if they fail.



---

## Chapter 2. Installing and configuring

IBM Intelligent Operations Center provides a deployment wizard that installs the environment required by the IBM Intelligent Operations Center. After deploying the environment and the IBM Intelligent Operations Center package, some additional configuration is required.

---

### Preparing for installation

Before deploying the IBM Intelligent Operations Center, understand the IBM Intelligent Operations Center system configuration and ensure that the prerequisites are met for the environment.

#### Related tasks:

“Installing the solution” on page 15

Installing the IBM Intelligent Operations Center involves several steps. A deployment wizard is provided to deploy and install the required environment and the IBM Intelligent Operations Center package.

### System configuration

The IBM Intelligent Operations Center installs and configures an environment with production servers and one server used during the installation process.

The IBM Intelligent Operations Center 1.0 deployment wizard installs and configures an environment with six production servers and one server used during the installation process.

**Fix Pack 1** The IBM Intelligent Operations Center 1.0 Fix Pack 1 must be installed on top of an existing IBM Intelligent Operations Center 1.0 environment. An additional server is required to install and run the IBM Intelligent Operations Center 1.0 Fix Pack 1. A temporary installation management server is also required during installation.

### Installation management server

The installation management server is used by the IBM Intelligent Operations Center installer. It is not used in the production environment. The installation management server contains the installation and configuration scripts used to deploy the other IBM Intelligent Operations Center servers.

### Access server

The access server provides security for the IBM Intelligent Operations Center solution. The access server contains the products, components, or feature packs shown in Table 2.

*Table 2. Access server contents*

Product, component, or feature pack	Default ports defined during installation
Tivoli Access Manager WebSEAL 6.1	HTTP service: port 80

### Application and integration server

The application and integration server provides application services for the IBM Intelligent Operations Center solution. The application and integration server contains the products, components, or feature packs shown in Table 3 on page 10.

Table 3. Application and integration server contents

Product, component, or feature pack	Default ports defined during installation
Model manager capability in IBM Integrated Information Core 1.4.0.1	WebSphere Application Server Admin console: port 9063 Web server: port 9082
WebSphere Message Broker 7.0.0.1	None
WebSphere MQ 7.0.1.3	WebSphere MQ Listener: port 1414
WebSphere Application Server Network Deployment 7.0.0.13	WebSphere Application Server Admin console: port 9060
<b>Fix Pack 1</b> WebSphere Application Server Network Deployment 7.0.0.19	HTTP server: port 9080
DB2 Enterprise Server Edition 9.7.0.4	Port 50000
Web 2.0 Feature Pack for WebSphere Application Server 1.0.1	None

## Portal server

The portal server provides user interface services for the IBM Intelligent Operations Center solution. When the IBM Intelligent Operations Center is installed the portal server contains the products, components, or feature packs shown in Table 4.

Table 4. Portal server contents

Product, component, or feature pack	Default ports defined during installation
IBM HTTP Server 7.0.0.0	HTTP service: port 8080 Admin: port 8008
WebSphere Portal Enable 7.0	Admin console: port 10001
<b>Fix Pack 1</b> WebSphere Portal Enable 7.0.0.2	Portal server: port 10039
Lotus Sametime Entry 8.5.1	SMTP service: port 25 HTTP service: port 81 LDAP service: port 389 NRPC service: port 1352 Messaging service: port 1533
Lotus Domino 8.5.1	SMTP service: port 25 HTTP service: port 81 LDAP service: port 389 NRPC service: port 1352 Messaging service: port 1533
IBM ILOG JViews Enterprise 8.7	None
DB2 Enterprise Server Edition 9.7.0.4	Port 50000

## Analytic server

The analytic server provides data analysis services for the IBM Intelligent Operations Center solution. The analytic server contains the products, components, or feature packs shown in Table 5 on page 11.

Table 5. Analytic server contents

Product, component, or feature pack	Default ports defined during installation
IBM Cognos Business Intelligence 10.1	WebSphere Application Server Admin console: port 9061 HTTP for WebSphere Application Server: ports 9081, 9082, 9083
IBM ILOG CPLEX Optimization Studio 12.2	None
IBM WebSphere Business Monitor 7.0.0.3	WebSphere Application Server Admin console: port 9060 HTTP server: port 9080
WebSphere Application Server Network Deployment 7.0.0.13 <b>Fix Pack 1</b> WebSphere Application Server Network Deployment 7.0.0.19	WebSphere Application Server Admin console: port 9060 HTTP server: port 9080
DB2 Enterprise Server Edition 9.7.0.4	Port 50000

## Event and management server

The event and management server manages events handled by the IBM Intelligent Operations Center solution. The event and management server contains the products, components, or feature packs shown in Table 6.

Table 6. Event and management server contents

Product, component, or feature pack	Default ports defined during installation
Tivoli Directory Server 6.2.0.1 <b>Fix Pack 1</b> Tivoli Directory Server 6.2.0.3	dsrdbm01 instance: port 389 itimldap instance: port 10389
Tivoli Directory Integrator 7.1	Port 52562
Tivoli Access Manager 6.1	Policy server: port 7135 Authorization server: port 7136
Tivoli Identity Manager 5.1.0.0	WebSphere Application Server Admin console: port 9061 HTTP server: port 9081
IBM Tivoli Monitoring 6.2.2.1	TEMS: port 1918 TEPS: port 1920
Tivoli Composite Application Manager 6.2.4	None
Tivoli Netcool/Impact 5.1.1	Command line: port 2000 Memory DB: port 5435
Tivoli Netcool/OMNIBUS 7.3.0	Object server: port 4100 Process agent: port 4200
WebSphere Application Server Network Deployment 7.0.0.13 <b>Fix Pack 1</b> WebSphere Application Server Network Deployment 7.0.0.19	WebSphere Application Server Admin console: port 9060 HTTP server: port 9080

Table 6. Event and management server contents (continued)

Product, component, or feature pack	Default ports defined during installation
WebSphere Application Server 6.0.0.23 (for Tivoli Identity Manager use only)	WebSphere Application Server Admin console: port 9061 HTTP server: port 9081
DB2 Enterprise Server Edition 9.7.0.4	db2inst1 instance: port 50000 db2inst2 instance: port 50002

## Database server

The database server provides repository and modeling services for the IBM Intelligent Operations Center solution. When the IBM Intelligent Operations Center is installed the database server contains the products, components, or feature packs shown in Table 7.

Table 7. Access server contents

Product, component, or feature pack	Default ports defined during installation
DB2 Enterprise Server Edition 9.7.0.4	Port 50000

### Fix Pack 1

## Tivoli Service Request Manager server

The Tivoli Service Request Manager server provides workflow and resource management services for events and incidents in the IBM Intelligent Operations Center solution. When the IBM Intelligent Operations Center 1.0 Fix Pack 1 is installed, the Tivoli Service Request Manager server contains the products, components, or feature packs shown in Table 8.

Table 8. Tivoli Service Request Manager server contents after Fix Pack 1 installation

Product, component, or feature pack	Default ports defined during installation
IBM HTTP Server 7.0.0.0	HTTP service: port 8080 Admin: port 8008
DB2 Enterprise Server Edition 9.7.0.4	Port 50000
WebSphere Application Server 6.1.0.2.9	WebSphere Application Server Admin console: port 9060 HTTP server: port 9080
Tivoli Service Request Manager Version 7.2.1	Port 9080

### Related concepts:

“What’s new in the fix pack?” on page 6

The IBM Intelligent Operations Center 1.0 Fix Pack 1 delivers stability improvements, upgrades to components, and system-monitoring infrastructure.

“Preparing to install the fix pack” on page 35

Before installing the IBM Intelligent Operations Center 1.0 Fix Pack 1, understand the system configuration, and ensure that the requirements and prerequisites are met.

## Hardware requirements

Each IBM Intelligent Operations Center server and client must meet the recommended hardware requirements.

## Server requirements

Each server must have an x86 64-bit processor including one of the following processors:

- AMD 64-bit processors
- Intel Extended Memory 64 Technology (EM64T) processors

Each IBM Intelligent Operations Center server requires the processors, memory, and hard disk space shown in Table 9.

Table 9. IBM Intelligent Operations Center server requirements

Server	Number of processors	Memory	Hard disk
Access server	4	16 GB	80 GB
Analytic server	8	16 GB	80 GB
Application and integration server	8	16 GB	80 GB
Database server	8	16 GB	80 GB
Event and management server	8	16 GB	80 GB
Portal server	8	16 GB	80 GB
Installation management server	2	8 GB	80 GB

### Notes:

- The /tmp folder on the installation management server must have at least 35 GB of available space.
- Additional hardware might be required if you plan on using Tivoli Service Request Manager with the IBM Intelligent Operations Center 1.0.

### Fix Pack 1

The additional server for the IBM Intelligent Operations Center 1.0 Fix Pack 1 requires the processors, memory, and hard disk space shown in Table 10.

Table 10. Requirements for the additional server of the IBM Intelligent Operations Center 1.0 Fix Pack 1

Server	Number of processors	Memory	Hard disk
Tivoli Service Request Manager	4	16 GB	80 GB

**Note:** Define swap space for each server to be twice the amount of the physical memory. For example, if a server has 16 GB memory, define 32 GB of swap space.

## Client requirements

Each client accessing the IBM Intelligent Operations Center must meet the following hardware requirements:

- A monitor with a minimum 1280 x 800 resolution
- 2 GB memory
- Network access with sufficient bandwidth for complex web client generation and continuous data updates

**Related concepts:**

“Installing Tivoli Service Request Manager” on page 23

Tivoli Service Request Manager can optionally be used with the IBM Intelligent Operations Center to manage incidents.

“Preparing to install the fix pack” on page 35

Before installing the IBM Intelligent Operations Center 1.0 Fix Pack 1, understand the system configuration, and ensure that the requirements and prerequisites are met.

## Software requirements

Each IBM Intelligent Operations Center server and client must meet the minimum software requirements.

### Operating systems

**Important:** Before installing the IBM Intelligent Operations Center, the IBM Intelligent Operations Center servers must have the following installed. No other software should be installed on the servers.

- 64-bit Red Hat Enterprise Linux 5 Update 5 with the Secure Shell (SSH) service installed and open

Also, in order to complete the single sign-on configuration required by the IBM Lotus Sametime portlet, a Windows system running Lotus Notes® Client 8.5.1 on the portal server is required.

### IBM Lotus Sametime

The Lotus Notes Client 8.5.1 client is included in the IBM Intelligent Operations Center package. Install the Lotus Notes Client on the portal server using the information in the Lotus Domino and Lotus Notes Information Center.

### Required downloads

You must download the following updates. These updates must be installed before deploying the solution.

- PO00001 implements fixes necessary for the IBM Intelligent Operations Center application
- PO00002 upgrades DB2 Enterprise Server Edition to Fixpack 4 and implements a number of infrastructure fixes

Follow the instructions provided in the download.

### Supported browsers

Clients accessing the IBM Intelligent Operations Center must have one of the following browsers:

- Internet Explorer 8.x (32-bit and 64-bit)
- Mozilla Firefox 3.0, 3.5 or 3.6

### Tivoli Service Request Manager

Additional software might be required if you plan on using Tivoli Service Request Manager with the IBM Intelligent Operations Center.

### Related concepts:

“Installing Tivoli Service Request Manager” on page 23

Tivoli Service Request Manager can optionally be used with the IBM Intelligent Operations Center to manage incidents.

“Preparing to install the fix pack” on page 35

Before installing the IBM Intelligent Operations Center 1.0 Fix Pack 1, understand the system configuration, and ensure that the requirements and prerequisites are met.

### Related information:

 Lotus Domino and Lotus Notes Information Center

 PO00001 Fix Download

 PO00002 Fix Download

## Media packaging

IBM Intelligent Operations Center can be ordered as a package of DVDs or can be obtained through Passport Advantage®.

The product number is 5725-D69.

### Related information:

 Passport Advantage

---

## Installing the solution

Installing the IBM Intelligent Operations Center involves several steps. A deployment wizard is provided to deploy and install the required environment and the IBM Intelligent Operations Center package.

### Before you begin

The IBM Intelligent Operations Center requires seven servers. These servers can be physical hardware servers, virtual machines running VMware, or servers in the cloud. Six of these servers are used in the production environment with the seventh being used only during the installation process.

Before installing IBM Intelligent Operations Center, make sure that the servers meet the hardware and software requirements.

Determine the administrator user ID and password for each server. These user IDs and passwords must be specified in the deployment wizard.

The IBM Intelligent Operations Center deployment wizard defines several user IDs and passwords during the deployment process. Before starting, determine the user IDs and passwords to be defined. The user IDs and password defined by the deployment wizard are:

- The root administrator user ID and password for the installation management server.
- The WebSphere Portal administrator ID and password.

### About this task

Installation of the IBM Intelligent Operations Center requires the following major steps:

1. Preparing the seven servers.
2. Copying the product images shipped with the IBM Intelligent Operations Center installation media to a temporary location.

3. Copying the IBM Intelligent Operations Center installation files to a temporary location
4. Running the IBM Intelligent Operations Center deployment wizard to install and configure the middleware required by the IBM Intelligent Operations Center solution and deploy the IBM Intelligent Operations Center.

**Related concepts:**

“Preparing for installation” on page 9

Before deploying the IBM Intelligent Operations Center, understand the IBM Intelligent Operations Center system configuration and ensure that the prerequisites are met for the environment.

“Post-installation configuration” on page 24

After deploying IBM Intelligent Operations Center, additional steps are required to configure the solution.

**Related tasks:**

“Verifying the solution installation” on page 33

You can verify that the IBM Intelligent Operations Center is correctly installed and configured.

## Preparing the servers

Before you begin the installation, first prepare the servers that the IBM Intelligent Operations Center will be installed on.

### Before you begin

A Domain Name System (DNS) server is recommended, but not necessary. If you do not have a DNS server, you can register host names in a local hosts file, for example, `\etc\hosts`. Use the example in this topic to ensure that you configure your local hosts file correctly.

Before installing the IBM Intelligent Operations Center, you are recommended to use the installation prerequisites checking tool to verify that the installation prerequisites are met. If you do not have a local DNS server, the tool identifies that as a missing prerequisite. The prerequisite is flagged even if you have a consistent local hosts file across all your servers so that they can communicate with each other.

**Note:** For Simplified Chinese in Cognos reports, when installing the IBM Intelligent Operations Center, set to Simplified Chinese the locale of the server designated to be the analytic server.

### About this task

To prepare servers in advance of installing the IBM Intelligent Operations Center, complete the following procedure. By completing the steps, you can avoid or eliminate errors identified by the prerequisite checking that takes place during the installation process.

### Procedure

1. Make sure that the Linux Distribution is Red Hat Enterprise Server.
2. Disable any firewalls and SELinux. Then restart the systems. You can enable firewalls after the installation completes.
3. To ensure that the servers can communicate with each another, each local hosts file must contain the names of all the other servers. See the example hosts file at the end of this procedure.
4. To verify server communication, ping each server with the fully-qualified name. You can also test the connections during the installation process. **Fix Pack 1** This connectivity test is done automatically by the installer during the installation of the IBM Intelligent Operations Center 1.0 Fix Pack 1.
5. Make sure that either the host name of each server is identical to the host name registered on the DNS server, or to the host name registered in the `/etc/hosts` file.
  - a. To check the host name of the server as registered either on the DNS server, or in the local hosts file, enter the command: `nslookup $(hostname -i)`



- b. To query the value of the host name to check that the local host name is correctly configured, enter the command: `hostname -f`

**Note:** The host names are case-sensitive.

6. If the host name is incorrect, complete the following steps:
  - a. Enter the following command: `hostname short_host_name`. For example: `hostname server1`
  - b. In the `/etc/sysconfig/network` file, modify or insert the following line:  
`HOSTNAME=short_host_name`
7. Make sure that the fully-qualified host name and the short host name are not mapped to `127.0.0.1` in the `/etc/hosts` file.
8. Make sure that each entry in the `/etc/hosts` file has the following format:  
*ip\_address fully-qualified\_host\_name short\_host\_name*  
  
For example: `192.168.1.101 server1.ibm.com server1`
9. Make sure that 30-GB disk space is available in both the `/tmp` directory and the `/opt` directory, so that a total of 60-GB disk space is available on the server.
10. Set the open file limit to be greater than 10000. The command to check that the open file limit is: `ulimit -n`. If the limit is not equal to 10000, it can be set using the command: `ulimit -n 10000`.
11. Enable Internet Protocol Version 6 (IPV6). Use the following commands to enable IPV6:  
`modprobe ipv6`  
`lsmod | grep ipv6`
12. Configure the password policy correctly. For more detail on modifying the password policy before installation, see the link at the end of the topic.
13. Allow root and other users to use Secure Shell (SSH). To enable password authentication and root user access between the operating system Red Hat Enterprise Linux and other SSH targets, complete the following steps:
  - a. On the target servers, edit the `/etc/ssh/sshd_config` file:
    - Delete the line with `AllowUsers`
    - Set the value of the parameter `PasswordAuthentication` to `yes`
    - Set the value of the parameter `PermitRootLogin` to `yes`
  - b. To stop and restart the SSH daemon, enter the following commands:  
`/etc/init.d/sshd stop`  
`/etc/init.d/sshd start`
14. Set all servers to have the same time and date as indicated by the Linux operating system.
15. Do not use a soft link for `/tmp`. A soft link means that `/tmp` is not the actual directory, but points to another directory. You can check if this is the case by running the command: `ls -la/`. Look for a line similar to: `drwxrwxrwt 21 root root 12288 Feb 10 11:12 tmp` If the `d` at the start here is a `l` instead, then `/tmp` is a soft link. For example, the code would be similar to: `lrwxrwxrwx 1 root root 10 Feb 23 2011 tmp -> root/tmp`. If this is the case, then you can run the command: `mv /tmp /tmp_old`  
`mkdir /tmp`

## Example

If there is no DNS and the host name is registered in the `/etc/hosts` file, follow the example provided here to write the `/etc/hosts` file. Note in the example how the local host is mapped to `127.0.0.1`, the host name is mapped to the IP address, and the fully-qualified host name is written before the short host name. The simplest way to ensure that the `/etc/hosts` configuration is consistent across all servers is to create and edit the file as shown in this example. Then, upload this file to all the servers.

```
127.0.0.1      localhost.localdomain localhost
192.168.1.101  server1.ibm.com server1
192.168.1.102  server2.ibm.com server2
192.168.1.103  server3.ibm.com server3
```

192.168.1.104	server4.ibm.com	server4
192.168.1.105	server5.ibm.com	server5
192.168.1.106	server6.ibm.com	server6
192.168.1.107	server7.ibm.com	server7
192.168.1.108	server8.ibm.com	server8

#### Related concepts:

“Preparing to install the fix pack” on page 35

Before installing the IBM Intelligent Operations Center 1.0 Fix Pack 1, understand the system configuration, and ensure that the requirements and prerequisites are met.

#### Related tasks:

“Checking installation prerequisites” on page 19

During the installation of IBM Intelligent Operations Center, errors or warnings might be displayed if the prerequisites are not met on all of the six target servers. Run the installation prerequisites checking tool to verify that the installation prerequisites are satisfied.

#### Related information:



Modifying the password policy before installation

## Copying files required to install and deploy the solution

The files required to install and deploy the IBM Intelligent Operations Center need to be copied to servers before running the deployment wizard.

### Procedure

1. Obtain the IBM Intelligent Operations Center media or downloads.
2. Copy the files on the IBM Intelligent Operations Center media and the IBM Intelligent Operations Center download to the installation management server. The files should be placed in a single directory, for example, /images.

## Extracting installation files and installing dependencies

After copying the required files to a temporary location, extract the installation files. Then install the dependencies before deploying the IBM Intelligent Operations Center.

### Procedure

1. On the installation management server, navigate to the directory where the IBM Intelligent Operations Center files were copied.
2. Extract the IBM Intelligent Operations Center files to the installation management server. Place the extracted files in a single directory, for example, /images. You can use the following commands to extract an image file, for example:

```
# tar xvf CI1WJEN.tar
# mkdir /mnt/cdrom
# mount -o loop CI1WJEN.iso /mnt/cdrom/
# cp /mnt/cdrom/* /images/
```

3. Extract the downloaded IBM Intelligent Operations Center update files to the installation management server. Place the extracted files in the same directory as the files mentioned in the previous step, for example, /images.
4. Extract IOC\_Installer\_XXXXXXXX-XXXX.tar.gz to a folder on the installation management server, for example, /installer by running the following command:  
# tar zxvf IOC\_Installer\_XXXXXXXX-XXXX.tar.gz -C /installer/  
XXXXXXXX-XXXX is a unique number indicating the build level.
5. Obtain the libXp-1.0.0-8.i386.rpm file from the Red Hat website and copy the file to the portal server.
6. To install the libXp-1.0.0-8.i386.rpm file on the portal server, run the following commands:

```
-bash-3.2# rpm -i libXp-1.0.0-8.i386.rpm
-bash-3.2# rpm -qa | grep libXp
libXp-1.0.0-8
```

7. On the Red Hat website, obtain the following files and copy them to the analytic server:

```
compat-libstdc++-33-3.2.3-61.i386.rpm
kernel-headers-2.6.18-238.el5.i386.rpm
compat-glibc-headers-2.3.4-2.26.i386.rpm
compat-glibc-2.3.4-2.26.i386.rpm
libXmu-1.0.2-5.i386.rpm
libXp-1.0.0-8.i386.rpm
openmotif22-2.2.3-18.i386.rpm
```

8. To install the files on the analytic server, run the following commands:

```
-bash-3.2# rpm -ivh compat-libstdc++-33-3.2.3-61.i386.rpm
-bash-3.2# rpm -ivh kernel-headers-2.6.18-194.el5.i386.rpm
-bash-3.2# rpm -ivh compat-glibc-headers-2.3.4-2.26.i386.rpm
-bash-3.2# rpm -ivh compat-glibc-2.3.4-2.26.i386.rpm
-bash-3.2# rpm -ivh libXmu-1.0.2-5.i386.rpm
-bash-3.2# rpm -ivh libXp-1.0.0-8.i386.rpm
-bash-3.2# rpm -ivh openmotif22-2.2.3-18.i386.rpm
```

#### Related concepts:

“Preparing to install the fix pack” on page 35

Before installing the IBM Intelligent Operations Center 1.0 Fix Pack 1, understand the system configuration, and ensure that the requirements and prerequisites are met.

#### Related information:

 Red Hat

## Checking installation prerequisites

During the installation of IBM Intelligent Operations Center, errors or warnings might be displayed if the prerequisites are not met on all of the six target servers. Run the installation prerequisites checking tool to verify that the installation prerequisites are satisfied.

### Before you begin

Before you run the installation prerequisites checking tool, ensure that OpenSSH version 4.4 or later is installed and enabled on the target servers. OpenSSH version 4.4, and later versions, contain security enhancements that are not available in earlier versions.

To enable password authentication and root user access between the installation prerequisites checking tool, the operating system, Red Hat Enterprise Linux, and other SSH targets; see the related task linked at the end of the topic.

### About this task

Run the installation prerequisites checking tool on the same server that you designated to run the IBM Intelligent Operations Center installer. Use the following procedure to install and run the installation prerequisites checking tool:

#### Procedure

1. Create a directory called *tool\_root*.
2. Obtain the installation prerequisites checking tool, see the related information link at the end of the topic.

3. Extract the `precheck.tar.gz` package from the IBM Intelligent Operations Center installation package to the `tool_root` directory.
4. To download and install the JRE version 6.0 or later, choose one of the following options:
  - Download and install the IBM Java SE JRE version 6.0 or later. To be able to download the IBM Java SE JRE from the IBM developerWorks site, you must have an IBM ID. See the related information link at the end of the topic.
  - Download and install the Sun JRE version 6.0 or later, see the related information link at the end of the topic.
5. Assign the correct value to `JAVA_HOME`. For example, enter the following command: 

```
> export JAVA_HOME=/opt/ibm/ibm-java-x86_64-60/jre
```
6. Copy the `tool_root/resource/precheck.properties` file and, in the copied file, update the host name, account, and password for each of the six servers in the IBM Intelligent Operations Center standard topology.
7. To verify the installation prerequisites, enter the following commands:

```
cd tool_root/ioc/bin
./precheck.sh prop_file_path
```

The variable `tool_root` is the directory containing the installation prerequisites checking tool package. The value of `prop_file_path` is `tool_root/resource/precheck.properties`, which is the file path for the `precheck.properties` file that you copied and updated in step 5.

## Results

If the installation prerequisites checking tool encounters an error, a message is issued. The warning and error messages are also listed in `tool_root/ioc/README.txt`.

### Related concepts:

“CHK: Installation prerequisite checking messages” on page 132


Use the information in this section to understand and respond to error, warning, and informational messages generated during the installation prerequisite checking process.

### Related tasks:

“Preparing the servers” on page 16

Before you begin the installation, first prepare the servers that the IBM Intelligent Operations Center will be installed on.

### Related information:

 [IBM Intelligent Operations Center installation prerequisites checking tool](#)

 [IBM Java SE JRE download](#)

 [Sun JRE download](#)

## Deploying the solution

The IBM Intelligent Operations Center provides a deployment wizard to install the IBM Intelligent Operations Center package.

### Before you begin

On the installation management server, navigate to the temporary directory where you copied the IBM Intelligent Operations Center installation files. Then navigate to the `disk1` directory. For example, if you copied the files to the `/images` directory, navigate to `/images/disk1`.

## Procedure

1. Run the following command:  

```
chmod +x -R *
```
2. To start the IBM Intelligent Operations Center deployment wizard, run the following command:  

```
./LinuxSetup
```

The first panel presented introduces the deployment wizard. Clicking **Help** on any panel provides general information about the deployment wizard; not specifics about the IBM Intelligent Operations Center deployment.

3. Click **Next**.
4. Select the task appropriate for your installation. There are two options:
  - The **Base Architecture Tasks** will install the products required by the IBM Intelligent Operations Center.
  - The **Intelligent Operations Center Tasks** will deploy the IBM Intelligent Operations Center solutions package.

To install the entire IBM Intelligent Operations Center solution, select both options.

**Important:** The IBM Intelligent Operations Center is not supported by IBM as a solution until both the **Base Architecture Tasks** and **Intelligent Operations Center Tasks** are completed.

5. Click **Next**.
6. If **Base Architecture Tasks** was selected, several panels will be displayed with tasks to install the products provided by the IBM Intelligent Operations Center. If you are installing the IBM Intelligent Operations Center for the first time on these servers, let all options default to selected. Some items might be disabled. You will be unable to select or deselect these items. If a product is already installed on the server, you can deselect the installation of the product. Click **Next** until all **Base Architecture Task** items have been reviewed and selected.
7. If **Intelligent Operations Center Task** was selected, an option to deploy the IBM Intelligent Operations Center package will be presented. If selected, the deployment wizard will also deploy the IBM Intelligent Operations Center package to the servers. Select whether the **Intelligent Operations Center Task** should be run and click **Next**.
8. In the next panels, complete the following:
  - a. Enter the host name or IP address, an administrator user ID, and the password for the ID for each target server. Operating system will be disabled since only Linux is supported by the IBM Intelligent Operations Center.
  - b. To test that the information provided is correct, click **Test connections**. If the connection test fails, solve the connection issue before proceeding.
  - c. To save the information for possible future use, select **Save this login information**.
  - d. Click **Next** after entering the data for each server.
9. The deployment wizard will define two user IDs and passwords during the deployment process. Define these user IDs and passwords in the next panels and click **Next** until the IDs have been defined:
  - An administrator ID and password for the IBM Intelligent Operations Center
  - An administrator ID and password for WebSphere Portal
10. A Summary Panel is displayed with all selected tasks and how long it will take to run each task. If you want to run all tasks, click **Deploy all**. A pop-up dialog is displayed and you can browse to select the location of the deployment package software to be installed, for example `/images`. If you want to run selected tasks, click **Deploy task** for each task you want to run. The selected deployment tasks are run. A message is displayed indicating if the deployment was completed successfully or if there were any errors. If there are errors, correct the errors and rerun the appropriate tasks.

11. If the **Intelligent Operations Center Task** was not selected, the IBM Intelligent Operations Center package can be deployed by rerunning the deployment wizard and selecting the **Intelligent Operations Center Task**. Alternately, the IBM Intelligent Operations Center package can be installed from a command line.

## Results

The IBM Intelligent Operations Center solution is installed.

### Related concepts:

“Hardware requirements” on page 12

Each IBM Intelligent Operations Center server and client must meet the recommended hardware requirements.

“Software requirements” on page 14

Each IBM Intelligent Operations Center server and client must meet the minimum software requirements.

“Media packaging” on page 15

IBM Intelligent Operations Center can be ordered as a package of DVDs or can be obtained through Passport Advantage.

“System configuration” on page 9

The IBM Intelligent Operations Center installs and configures an environment with production servers and one server used during the installation process.

### Related tasks:

“Deploying the package from a command line”

The IBM Intelligent Operations Center solution package can be deployed after the base architecture is deployed. If the deployment wizard is unable to completely deploy the IBM Intelligent Operations Center solutions package, or if the **Intelligent Operations Center Tasks** option was not selected in the deployment wizard, the IBM Intelligent Operations Center solutions package can be deployed from a command line.

## Deploying the package from a command line

The IBM Intelligent Operations Center solution package can be deployed after the base architecture is deployed. If the deployment wizard is unable to completely deploy the IBM Intelligent Operations Center solutions package, or if the **Intelligent Operations Center Tasks** option was not selected in the deployment wizard, the IBM Intelligent Operations Center solutions package can be deployed from a command line.

## Procedure

1. Log in to the event and management server as root. Optionally, log in to the event and management server as an administrator and use the **sudo** command to run the required commands if you are unable to log in as root.
2. Remove the `/opt/IBM/iss` directory.
3. Extract the `IOC.tar` file into the `/opt/IBM` directory. The files should be in the `/opt/IBM/iss` directory when extracted.
4. Navigate to the `/opt/IBM/ISP/ioc/binary` directory.  

```
-bash-3.2# cd /opt/IBM/ISP/ioc/binary/
```
5. Run this command:  

```
-bash-3.2# ./install.sh admin password
```

Where *admin* and *password* are the administrator user ID and password specified when the IBM Intelligent Operations Center deployment wizard was run.
6. If an error is displayed, check the `install.log` file for details. Correct any errors. Rerun the command.

## What to do next

Log in to the portal on the portal server to verify that IBM Intelligent Operations Center has been successfully deployed. The **Intelligent Operations Center** page should be displayed.

## Running specific deployment tasks

Specific deployment tasks can be run to reinstall parts of the solution, or to run a deployment task that might have failed.

To run one or more deployment tasks, run the deployment wizard and select the tasks to be run.

### Related tasks:

“Deploying the solution” on page 20

The IBM Intelligent Operations Center provides a deployment wizard to install the IBM Intelligent Operations Center package.

## Installing Tivoli Service Request Manager

Tivoli Service Request Manager can optionally be used with the IBM Intelligent Operations Center to manage incidents.

Tivoli Service Request Manager is provided with the IBM Intelligent Operations Center media package. It is not installed by the IBM Intelligent Operations Center deployment wizard.

**Restriction:** The version of Tivoli Service Request Manager provided with the IBM Intelligent Operations Center package can be used only with the IBM Intelligent Operations Center. It cannot be used stand-alone or with any other applications.

For system requirements and installation instructions for Tivoli Service Request Manager, see the Tivoli Service Request Manager information center. Tivoli Service Request Manager should be installed on a separate server from the IBM Intelligent Operations Center servers.

### Related concepts:

“System configuration” on page 9

The IBM Intelligent Operations Center installs and configures an environment with production servers and one server used during the installation process.

“Hardware requirements” on page 12

Each IBM Intelligent Operations Center server and client must meet the recommended hardware requirements.

“Software requirements” on page 14

Each IBM Intelligent Operations Center server and client must meet the minimum software requirements.

### Related information:



Tivoli Service Request Manager information center

## Installing tools provided with the solution

Toolkits and development tools are included with the IBM Intelligent Operations Center. These are used when customizing the IBM Intelligent Operations Center.

With the exception of Rational® Application Developer, these are provided on the IBM Intelligent Operations Center Developer's Toolkit DVD or image. Rational Application Developer is included with the IBM Intelligent Operations Center on separate DVDs or images.

## Lotus Sametime Client

For information on installing and using the Lotus Sametime Client , see the Lotus Domino and Lotus Notes information center.

## WebSphere Message Broker Toolkit

For information on installing and using the WebSphere Message Broker Toolkit, see the WebSphere Message Broker information center.

## IBM WebSphere Business Monitor Development Toolkit

For information on installing and using the IBM WebSphere Business Monitor Development Toolkit, see the IBM WebSphere Business Monitor information center.

## Rational Application Developer

For information on installing and using Rational Application Developer, see the Rational Application Developer information center.

### Related information:

 [Lotus Domino and Lotus Notes information center](#)

 [WebSphere Message Broker information center](#)

 [IBM Business Monitor information center](#)

 [Rational Application Developer information center](#)

---

## Post-installation configuration

After deploying IBM Intelligent Operations Center, additional steps are required to configure the solution.

So IBM Lotus Sametime can be used with WebSphere Portal, single sign-on must be configured. Single sign-on must also be configured between IBM Lotus Sametime and Tivoli Access Manager WebSEAL.

### Related tasks:

“Installing the solution” on page 15

Installing the IBM Intelligent Operations Center involves several steps. A deployment wizard is provided to deploy and install the required environment and the IBM Intelligent Operations Center package.

## Setting the WebSphere Portal session timeout value

The WebSphere Portal session timeout value needs to be set to stop a user from being logged out during a session. This value must match the Tivoli Access Manager WebSEAL cache settings timeout value.

### Procedure

1. Open a WebSphere Application Server administrative console at `http://server:port/ibm/console`. Replace *server* and *port* with the default values or the values that have been configured, whichever applies. For more information about the default port numbers, see “System configuration” on page 9.
2. Click **Servers > Server Type - WebSphere Application Servers > WebSphere Portal > Session management**.
3. For **Session timeout**, select **Set timeout** and enter the required timeout value in minutes. For example, 540 minutes (9 hours).
4. Click **OK**.
5. Save the changes to the master configuration.



6. To restart WebSphere Portal, run the following commands:

```
/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh WebSphere_Portal  
/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal
```

**Related concepts:**

“System configuration” on page 9

The IBM Intelligent Operations Center installs and configures an environment with production servers and one server used during the installation process.

**Related tasks:**

“Setting the Tivoli Access Manager WebSEAL session cache settings timeout value”

The Tivoli Access Manager WebSEAL session cache settings timeout value must be set to the same value as the WebSphere Portal session timeout.

## Setting the Tivoli Access Manager WebSEAL session cache settings timeout value

The Tivoli Access Manager WebSEAL session cache settings timeout value must be set to the same value as the WebSphere Portal session timeout.

### Procedure

1. Log in to the access server as root.
2. In a terminal session, edit the `/opt/pdweb/etc/webseald-default.conf` file and change the timeout value in the SESSION CACHE SETTINGS section to be the same as the session timeout for WebSphere Portal.

**Important:** The SESSION CACHE SETTINGS timeout value is specified in seconds. The WebSphere Portal session timeout is specified in minutes. If the WebSphere Portal session timeout is 540 minutes (9 hours), the corresponding SESSION CACHE SETTINGS timeout value would be 32400.

3. To restart Tivoli Access Manager WebSEAL run the following command:

```
/usr/bin/pdweb restart
```

**Related tasks:**

“Setting the WebSphere Portal session timeout value” on page 24

The WebSphere Portal session timeout value needs to be set to stop a user from being logged out during a session. This value must match the Tivoli Access Manager WebSEAL cache settings timeout value.

## Configuring single sign-on

IBM Intelligent Operations Center uses Tivoli Directory Server as its LDAP server to store user information. For proper interaction with IBM Lotus Sametime, single sign-on must be enabled for the solution.

In the IBM Intelligent Operations Center solution, Tivoli Access Manager WebSEAL authenticates users when accessing the IBM Intelligent Operations Center.

Single sign-on within the solution requires configuration in two areas:

- Configuring single sign-on between WebSphere Portal and IBM Lotus Sametime.
- Configuring single sign-on between Tivoli Access Manager WebSEAL and IBM Lotus Sametime.

A junction is used to connect Tivoli Access Manager WebSEAL, WebSphere Portal, and WebSphere Application Server Network Deployment through the WebSphere Trust Association Interceptor interface. A junction is also used to connect Tivoli Access Manager WebSEAL and IBM Lotus Sametime to enable use of IBM Lotus Sametime in a browser.

Single sign-on between WebSphere Portal, IBM Lotus Sametime, and other servers uses an IBM LTPA (Lightweight Third Party Authentication) token to share user credentials.

## Configuring IBM Lotus Sametime and WebSphere Portal single sign-on

Configure single sign-on between IBM Lotus Sametime and WebSphere Portal so IBM Lotus Sametime can be used with IBM Intelligent Operations Center.

### Before you begin

Before configuring single sign-on, the following must be successfully installed.

- The IBM Intelligent Operations Center base architecture
- The IBM Intelligent Operations Center solutions package
- The correct JRE for the IBM Lotus Sametime portlet.

You also must be able to access the following:

- WebSphere Portal at `http://portal_hostname:10039/wps/portal`
- IBM Lotus Sametime at `http://sametime_hostname.domain_name:81/`

Where *portal\_hostname* is the host name for WebSphere Portal, *sametime\_hostname* is the host name for IBM Lotus Sametime, and *domain\_name* is the domain name for IBM Lotus Sametime.

### Procedure

1. "Importing the WebSphere Portal SSO LTPA token"
2. "Verifying the configuration changes" on page 27

### Importing the WebSphere Portal SSO LTPA token:

Use the following procedure to import the WebSphere Portal SSO LTPA token into the Lotus Domino server.

### Procedure

1. Install the Lotus Notes Client 8.5.1 on a Windows system using the instructions in the Lotus Domino and Lotus Notes information center. When performing this install, ensure that you include the Domino Administrator.
  2. Copy the IBM Lotus Sametime administrator ID and the LTPA key file from the portal server to the system running the Lotus Notes Client. The default location of the administrator ID is `/local/notesdata/admin.id`. The default location of the LTPA key file is `/opt/IBM/iss/portal.ltpa`.
  3. Open the Lotus Domino Administrator Client. Set **name** to notes admin and **Domino server** to your portal host name.
  4. Switch to the `admin.id` file using **File > Security > Switch ID**.
  5. Log in using the administrator ID copied from the portal server.
  6. Click **File > Open > Lotus Notes Application**, select `default/IBM` in the list and open the directory database, `names.nsf`.
  7. Click **Web > Web configurations > Web SSO Configurations > Web SSO Configuration for Ltpa Token**.
  8. Click **Edit Document**.
  9. Click **Keys... > Import WebSphere LTPA Key**.
  10. Click **OK** to overwrite the configuration.
  11. Enter the full path to the LTPA file and the LTPA filename on the Windows system.
  12. Enter the password for the LTPA file set when the LTPA file was exported.
  13. Set **Map names in LTPA tokens** to **Enabled**.
  14. Set **DNS Domain** to the domain name set in WebSphere Portal. For example, `.yourco.com`.
  15. Click **Save & Close**.
  16. Restart the IBM Lotus Sametime server on the portal server as follows:
- 26 IBM Intelligent Operations Center: IBM Intelligent Operations Center Product Documentation

- a. Log in to the portal server as root.
- b. To stop the IBM Lotus Sametime server, run the following commands:

```
su - notes
cd /local/notesdata
/opt/ibm/lotus/bin/server -q
```

- c. Wait until you see the message Server shutdown complete and start the IBM Lotus Sametime server with the commands:

```
su - notes
cd /local/notesdata
nohup /opt/ibm/lotus/bin/server &
```

17. To stop the WebSphere Portal server, run the following command on the portal server as user root:  
/opt/IBM/WebSphere/wp\_profile/bin/stopServer.sh WebSphere\_Portal
18. To remove all WebSphere Portal temporary files, run the following command:  
rm -rf /opt/IBM/WebSphere/wp\_profile/wstemp/
19. To start the WebSphere Portal server, run the following command on the portal server as user root:  
/opt/IBM/WebSphere/wp\_profile/bin/startServer.sh WebSphere\_Portal

#### Related information:



Lotus Domino and Lotus Notes information center

#### Verifying the configuration changes:

To verify your configuration changes, complete the following procedure.

##### Procedure

1. Open the IBM Intelligent Operations Center portal.
2. Go to the **Sametime Contact List**.
3. Confirm that the logged on user is displayed as online.

### Configuring IBM Lotus Sametime and Tivoli Access Manager WebSEAL single sign-on

Single sign-on must be configured for Tivoli Access Manager WebSEAL so IBM Lotus Sametime can be used with IBM Intelligent Operations Center.

##### Procedure

1. “Enabling HTTP tunneling”
2. “Modifying the stlinks.js file” on page 28
3. “Enabling a reverse proxy” on page 28
4. “Creating a Tivoli Access Manager WebSEAL junction” on page 29
5. “Restarting the IBM Lotus Sametime server” on page 30

#### Enabling HTTP tunneling:

To enable HTTP tunneling, complete the following procedure.

##### Procedure

1. On the Windows system, run the Lotus Domino Administrator. For information on running the Lotus Domino Administrator, see the Lotus Domino and Lotus Notes information center.
2. Click **File > Open > Lotus Notes Application**, select default/IBM and open the Sametime Configuration database, StConfig.nsf.
3. Select **All-By Form and Date**, double-click the item under the **CommunityConnectivity** section of the form to edit the values.

4. Change the **HTTP Tunneling Port** to 81.
5. Change the **HTTP Tunneling Host Name** to the IBM Lotus Sametime host name.
6. Make sure **Is HTTP Tunneling supported?** is true.
7. Open the **BroadcastGateway** document.
8. Change the **HTTP Tunneling Port** to 81.
9. Change the **HTTP Tunneling Host Name** to the IBM Lotus Sametime host name.
10. Make sure **HTTP Tunneling Support** is true.
11. Open the **MeetingServices** document.
12. Change the **HTTP Tunneling Port** to 81.
13. Change the **HTTP Tunneling Host Name** to the IBM Lotus Sametime host name.
14. Make sure **HTTP Tunneling Support Enabled** is true.
15. Close the tabs and save the changes.
16. In Lotus Domino Administrator open the **ICP Domain - default/IBM** tab, then open the **Configuration** tab.
17. Select the **Current Server Document** under the **Server** twistie.
18. Open the **Ports** tab.
19. Open the **Internet Ports** tab.
20. Open the **Web** tab.
21. Change **TCP/IP port number** to 8088.
22. Close the tabs and save the changes.
23. Edit the `/local/notesdata/sametime.ini` file.
24. Make sure `ConfigurationPort` is set to 8088 as follows.
 

```
ConfigurationPort=8088
```

#### Related information:



Lotus Domino and Lotus Notes information center

#### Modifying the `stlinks.js` file:

To modify the `stlinks.js` file, complete the following procedure.

#### Procedure

1. Edit the `/local/notesdata/domino/html/sametime/stlinks/stlinks.js` file.
2. Make sure the following values are set.

```
var ll_RProxyName="http://webseal_hostname";
var ll_AffinityId="junction";
isTAM_env = true;
racingConnTimeout = 5000;
```

Where `webseal_hostname` is the host name for Tivoli Access Manager WebSEAL and `junction` is the junction name to be created with Tivoli Access Manager WebSEAL.

3. Save the file.

#### Related tasks:

“Creating a Tivoli Access Manager WebSEAL junction” on page 29

To create the junction in Tivoli Access Manager WebSEAL, complete the following procedure.

#### Enabling a reverse proxy:

To enable a reverse proxy complete the following procedure.

## Procedure

1. Log in to the IBM Lotus Sametime Administration portal on the portal server. The username is notesadmin. The URL for the IBM Lotus Sametime Administration portal will be similar to the following. Replace *your\_sametime\_domain\_name* with the fully-qualified domain name appropriate to your installation.

```
http://your_sametime_domain_name:81/stcenter.nsf?Login
```

If there is a problem logging in using the preceding URL, clear the browser cache and log in using the following URL:

```
http://portal_server_domain_name:81
```

Click on **Administer the server**.

2. Click **Configuration > Connectivity**.
3. Under **Community Services Network** select **Enable the Sametime Connect for browsers client to try HTTP tunneling to the Community Server after trying other options**. Ensure the portal server host name is in the host name field. If this field is left blank, the service will bind to all the host names on the server. Enter 81 in the port number field.
4. Under **Reverse Proxy Support** select **Enable Reverse Proxy Discovery on the client**.
5. For **Server Alias (this is what the Reverse Proxy is using to forward HTTP(S) messages to the server)**, enter the name you will use when creating a Tivoli Access Manager WebSEAL junction, for example, st.
6. Click **Update**.

### Related tasks:

“Creating a Tivoli Access Manager WebSEAL junction”

To create the junction in Tivoli Access Manager WebSEAL, complete the following procedure.

### Creating a Tivoli Access Manager WebSEAL junction:

To create the junction in Tivoli Access Manager WebSEAL, complete the following procedure.

## Procedure

1. Copy the LTPA key from the portal server to the access server.
2. To log in to the Tivoli Access Manager WebSEAL pdadmin command console, on the access server, run the following command:

```
pdadmin -a sec_master -p password
```

3. On the access server, run the following command:

```
pdadmin> server task default-webseald-server_name create -t tcp -h sametime_host_name  
-p 81 -i -j -A -F path_to_LTPA_key -Z LTPA_key_password /st
```

Where:

- *server\_name* is the fully-qualified host name of the Tivoli Access Manager WebSEAL server.
- *sametime\_host\_name* is the IBM Lotus Sametime server host name on the portal server.
- *path\_to\_LTPA\_key* is the path where the LTPA key was copied to on the access server.
- *LTPA\_key\_password* is the password for the LTPA key file.

For example:

```
server task default-webseald-rhel21.yourco.com create -t tcp -h rhel21.yourco.com  
-p 81 -i -j -A -F /tmp/portal.ltpa -Z pw123456 /st
```

**Important:** Do not specify the `-w` parameter. Specifying `-w` might prevent some requests generated by IBM Lotus Sametime from being passed through the junction.

The LTPA key used in the junction is the same LTPA key used by the IBM Lotus Sametime server in its Web SSO Configuration document. The IBM Lotus Sametime LTPA key was specified when

configuring WebSphere Portal single sign-on. To see the default-webseald server name, use the command `pdadmin> server list` to print out the list of servers.

### Restarting the IBM Lotus Sametime server:

To restart IBM Lotus Sametime, complete the following procedure.

#### Procedure

1. To stop the IBM Lotus Sametime server, on the portal server, run the following commands:

```
su - notes
cd /local/notesdata
/opt/ibm/lotus/bin/server -q
```

2. To start the IBM Lotus Sametime server, on the portal server, run the following commands:

```
su - notes
cd /local/notesdata
nohup /opt/ibm/lotus/bin/server &
```

## Creating a WebSphere Application Server Network Deployment junction

You can deploy an application on the WebSphere Application Server Network Deployment. This is an optional task. To complete the task, you must create a junction and ACL for the WebSphere Application Server Network Deployment. To do this, use either a command line or the Tivoli Access Manager Web Portal Manager.

#### Related concepts:

“Managing a Tivoli Access Manager WebSEAL junction ACL” on page 56

To manage users and groups defined in the Tivoli Access Manager WebSEAL junction, an administrator can use commands or the Tivoli Access Manager Web Portal Manager.

### Creating a WebSphere Application Server Network Deployment junction using the command line

A standard junction and ACL can be created by running a series of commands.

#### Procedure

1. On the access server, log in to the Tivoli Access Manager WebSEAL server terminal using the following commands:

```
# pdadmin
login
```

Use `sec_master` for the user ID and enter the password.

2. Create a standard junction by running the following command:

```
server task default-webseald-WebSEAL_Host_Name create -b supply -c iv-creds -t tcp -h WAS_Host_Name -p WAS_Port /Junction_Name
```

3. Add another WebSphere Application Server to the same junction by running the following command:

```
server task default-webseald-WebSEAL_Host_Name add -h WAS_Host_Name -p WAS_Port /Junction_Name
```

4. Create an ACL by running the following command:

```
acl create ACL_Name
```

5. Attach the ACL to the junction by running the following command:

```
acl attach /WebSEAL/WebSEAL_Host_name/Junction_Name ACL_Name
```

### Creating a WebSphere Application Server Network Deployment junction using the Tivoli Access Manager WebSEAL Web Portal Manager

A standard junction and ACL can be created by using the Tivoli Access Manager WebSEAL Web Portal Manager.

## Procedure

1. Access the Tivoli Access Manager WebSEAL Web Portal Manager at the following URL:  
`http://events_and_management_server_hostname:9061/ibm/console`

Use `sec_master` for the user ID and enter the password.

2. Click **Tivoli Access Manager > Web Portal Manager > WebSEAL > List Junction**.
3. Login with `sec_master` as the user ID and enter the password.
4. Click **Create**.
5. Enter the following data.
  - Junction Point:** The name for the junction point. The name must begin with a slash (/).
  - Target Host:** The WebSphere Application Server host name.
  - TCP Port:** The WebSphere Application Server port number. This is normally 9080.
  - Client Identity Header:** Specify User Credential.
  - Type:** Specify Supply.
6. Click **Create**.
7. Add another WebSphere Application Server to the junction, by clicking **Add** on the List Junctions page. Then enter the WebSphere Application Server **Target Host** and **TCP Port** information.
8. Click **Create**.
9. Click **Tivoli Access Manager > Web Portal Manager > ACL**.
  - Use `sec_master` for the user ID and `password` for the password.
10. Click **Create**.
11. Enter a value for **ACL Name**.
12. Click **Create**.
13. Click **Tivoli Access Manager > Web Portal Manager > Object Space > Browse Object Space**.
  - Use `sec_master` for the user ID and `password` for the password.
14. Expand the **Object Space** view and goto `/WebSEAL/WebSEAL_hostname-default/junction_name`.
15. Select the `junction_name` created previously.
16. Click **Attach** next to the **ACL Attached** field.
17. Select the ACL name previously created from the list.
18. Click **Apply**.

## Configuring WebSphere Application Server Network Deployment for LTPA single sign-on

By default the IBM Intelligent Operations Center is configured to use the Tivoli Access Manager Trust Association Interceptor (TAI++) as the single sign-on solution for WebSphere Application Server Network Deployment. Alternately, Lightweight Third-Party Authentication (LTPA) can be used for WebSphere Application Server Network Deployment single sign-on.

### About this task

To use LTPA for single sign-on, the LTPA key must be imported into WebSphere Application Server Network Deployment.

## Procedure

1. On the portal server, find the LTPA key file. By default the file is `/opt/IBM/iss/portal.ltpa`.
2. Copy the LTPA key file to the application and integration server. For example, into the `/tmp` directory.

3. Log into the WebSphere Application Server Network Deployment console on the application and integration server. The URL will be similar to the following:

`http://hostname:9060/admin`

where *hostname* is the WebSphere Application Server Network Deployment host name.

4. Click **Security > Global Security > LTPA**.
5. Enter the LTPA key password in **Password** and **Confirm password**.
6. Enter the fully qualified file name where you copied the LTPA key file in step 2 on page 31 in **Fully qualified key file name**. For example, `/tmp/portal.ltpa`.
7. Click **Import keys**.
8. Click **Save** to save the configuration.
9. Click **System administration > Nodes**.
10. Click **Synchronize** to synchronize the key between WebSphere Application Server Network Deployment and the nodes.
11. Restart Deployment Manager, the node agent and servers.

## Enabling login redirection

Tivoli Access Manager WebSEAL needs to be configured to redirect the user to the default IBM Intelligent Operations Center portal after log in.

### About this task

When a user's session times out and Tivoli Access Manager WebSEAL re-authenticates the user, the user might not be properly redirected to the IBM Intelligent Operations Center after successful authentication.

To configure automatic redirection, complete the following procedure.

### Procedure

1. Log in to the access server.
2. In the `/opt/pdweb/etc` directory, edit the Tivoli Access Manager WebSEAL configuration file. The file name will be in the form `webseald-webseal_instance_name.config` where *webseal\_instance\_name* is the name of the Tivoli Access Manager WebSEAL instance.
3. In `[enable-redirects]`, remove the `#` character from before `forms-auth`.
4. For `login-redirect-page` specify the URL the user will be redirected to after login. Specify the URL as an IBM Intelligent Operations Center relative path. For example, `/wpsv70/wps/myportal`.
5. Save the changes.
6. To stop and restart the Tivoli Access Manager WebSEAL server, run the following command:  

```
pdweb restart
```

## Configuring the REST Services Gateway port and protocol

Change the REST Services Gateway protocol and port values for correct key performance indicator (KPI) processing.

### About this task

To configure the REST Services Gateway port and protocol, on the analytic server, use the WebSphere Application Server administrative console and the `qmwas` profile.

### Procedure

1. Open **Services > REST services > REST service providers > REST Services Gateway**.
2. Select **http://** for **Protocol**.



3. Enter 9080 for **Port**.
4. Save the changes.

## Deleting sample users

The IBM Intelligent Operations Center is shipped with sample users. For security reasons these users should be deleted after the IBM Intelligent Operations Center is installed.

### About this task

To delete the predefined users, complete the following steps

### Procedure

1. On the portal server, sign into WebSphere Portal.
2. On the **Administration** portal, click **Access > Users and Groups > All Authenticated Portal Users**.
3. Click the delete icon for the following users:
  - tdelorne
  - scollins
  - akelly

**Important:** Do not delete the following required users. If you delete them, IBM Intelligent Operations Center will not operate properly.

- wpsadmin
- wasadmin
- wpsbind
- admin
- notesadmin

### Related reference:

“Sample users” on page 49

During the deployment of the IBM Intelligent Operations Center, sample users are created.

---

## Verifying the solution installation

You can verify that the IBM Intelligent Operations Center is correctly installed and configured.

### About this task

After installing and configuring the IBM Intelligent Operations Center, complete the following procedure to verify that the solution is correctly installed and configured.

### Procedure

1. To check the status of the components, on the event and management server, run the following command:

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh status all admin_password
```

Where *admin\_password* is the IBM Intelligent Operations Center administrator password. The command returns results similar to the following output:

```
Executing query command.....completed.  
IBM DB2 Enterprise server for IBM Solutions Kit [ on ]  
IBM DB2 Enterprise server for Tivoli Identify Manager [ on ]  
IBM DB2 Enterprise server for Runtime [ on ]  
IBM DB2 Enterprise server for WebSphere Portal Extend [ on ]  
IBM DB2 Enterprise server for COGNOS [ on ]  
IBM DB2 Enterprise server for MIH [ on ]
```

```

IBM Tivoli Directory Server [ on ]
IBM Tivoli Access Manager Policy Server [ on ]
IBM Tivoli Access Manager Authorization Server [ on ]
IBM Tivoli Access Manager Web Portal Manager [ on ]
IBM Tivoli Access Manager WebSEAL [ on ]
IBM Tivoli Monitoring Enterprise Monitoring Server [ on ]
IBM Tivoli Monitoring Enterprise Portal Server [ on ]
IBM Solutions Kit Core Server [ on ]
IBM Tivoli Identity Manager [ on ]
IBM WebSphere Deployment Manager Server for Runtime [ on ]
IBM WebSphere Application Server for Runtime [ on ]
IBM HTTP Server [ on ]
IBM WebSphere Message Broker [ on ]
IBM Tivoli Netcool OMNIBus [ on ]
IBM Tivoli Netcool Impact [ on ]
IBM Lotus Sametime [ on ]
IBM Master Information Hub [ on ]
IBM COGNOS Business Intelligence [ on ]
IBM WebSphere Portal Extend [ off ]
IBM WebSphere Business Monitor [ on ]

```

Command completed successfully.

**Fix Pack 1** For the IBM Intelligent Operations Center 1.0 Fix Pack 1, the command returns results similar to the following output:

```

Executing query command.....completed.
IBM DB2 Enterprise server for Portal Server [ on ]
IBM DB2 Enterprise server for Application Server [ on ]
IBM DB2 Enterprise server for Runtime [ on ]
IBM DB2 Enterprise server for Analytics Server [ on ]
IBM DB2 Enterprise server for Management Server [ on ]
IBM DB2 Enterprise server for TSRM Server [ on ]
IBM Tivoli Directory Server [ on ]
IBM Tivoli Access Manager Policy Server [ on ]
IBM Tivoli Access Manager Authorization Server [ on ]
IBM Tivoli Access Manager Web Portal Manager [ on ]
IBM Tivoli Access Manager WebSEAL [ on ]
IBM WebSphere Message Broker [ on ]
IBM WebSphere Business Monitor [ on ]
IBM Solutions Kit Core Server [ on ]
IBM Tivoli Identity Manager [ on ]
IBM WebSphere Application Server for Runtime [ on ]
IBM HTTP Server [ on ]
IBM WebSphere Application Server for CPLEX [ on ]
IBM Tivoli Netcool OMNIBus [ on ]
IBM Tivoli Netcool Impact [ on ]
IBM Lotus Sametime [ on ]
IBM Master Information Hub [ on ]
IBM COGNOS Business Intelligence [ on ]
IBM WebSphere Portal Extend [ on ]
IBM Tivoli Service Request Manager [ on ]
IBM Tivoli Monitoring Enterprise Monitoring Server [ on ]
IBM Tivoli Monitoring Enterprise Portal Server [ on ]
Command completed successfully.

```

**Note:** Components with an off status are not running and must be started. Use the **IOControl** command to stop and then start all of the components. It is possible to start components individually, but this use of the command is not recommended. For more information about controlling components, see the related concept linked at the end of the topic.

2. Send test events from the IBM Intelligent Operations Center portal.
  - a. To log on as a user with administrator privileges use the URL where the IBM Intelligent Operations Center was installed. For example: `http://access_server_name/wpsv70/wps/myportal`.
  - b. Click **Intelligent Operations Center**. Verify that IBM Intelligent Operations Center portlets are correctly displayed.

- c. Click **Administration > Verification Tools > Sample event publisher**. Click **Submit Event** to send a sample non-KPI and a KPI event to the IBM Intelligent Operations Center.
- d. Click **Intelligent Operations Center > City-wide Operations**. In the Events portlet, verify that the sample non-KPI event is listed.
- e. Click **Intelligent Operations Center > City-wide Executive**. In the Status portlet, verify that the sample KPI event is listed.

**Related concepts:**

“Intelligent Operations Center - About” on page 97

Use the Intelligent Operations Center - About portlet to view details of the version of the IBM Intelligent Operations Center and the integrated IBM Smarter Cities Software Solutions that you have installed.

“Sample Publisher” on page 69

Use the Sample Publisher portlet to publish Common Alerting Protocol (CAP) events into the IBM Intelligent Operations Center.

“Controlling components with **IOControl**” on page 97

You can control or query the status of the IBM Intelligent Operations Center components by using the **IOControl** command.

**Related tasks:**

“Installing the solution” on page 15

Installing the IBM Intelligent Operations Center involves several steps. A deployment wizard is provided to deploy and install the required environment and the IBM Intelligent Operations Center package.

“Installing the fix pack” on page 41

Use the command line to install the IBM Intelligent Operations Center 1.0 Fix Pack 1.

---

## Verifying the publishing of CAP events

You can create sample events and publish Common Alerting Protocol (CAP) messages into the IBM Intelligent Operations Center.

For information on creating sample events and publishing sample CAP messages, see the link at the end of the topic.

**Related concepts:**

“Publishing CAP messages” on page 69

The IBM Intelligent Operations Center provides the Sample Publisher portlet as an automated test tool and provides additional publishing capabilities as a service.

---

## Installing and configuring the fix pack

### Fix Pack 1

The IBM Intelligent Operations Center 1.0 Fix Pack 1 is designed to be installed on top of an existing IBM Intelligent Operations Center 1.0 environment. Follow the instructions provided in this section of the information center.

## Preparing to install the fix pack

### Fix Pack 1

Before installing the IBM Intelligent Operations Center 1.0 Fix Pack 1, understand the system configuration, and ensure that the requirements and prerequisites are met.

## System configuration

When you install the fix pack the IBM Intelligent Operations Center 1.0 environment is reconfigured. One additional server is required to install and run the fix pack. The existing installation management server is required during the fix pack installation process.

The additional Tivoli Service Request Manager server provides workflow and resource management services for events and incidents in the IBM Intelligent Operations Center solution. For more details on the products, components, or feature packs installed on each server, see the related concept link at the end of the topic.

**Note:** You might have completed a manual installation of Tivoli Service Request Manager for IBM Intelligent Operations Center 1.0. In that case, you can choose the fix pack installation option to omit the installation and configuration of Tivoli Service Request Manager.

## Hardware and software requirements

To ensure that the fix pack installation is successful, make sure that the servers and clients meet the recommended hardware and software requirements. For more details on the requirements, see the related concept links at the end of the topic.

## Prerequisites

Before installing the IBM Intelligent Operations Center 1.0 Fix Pack 1, ensure that you complete the following prerequisites:

- Install the IBM Intelligent Operations Center 1.0 environment running either interim fix PO00002 or PO00007. You may also install interim fix PO00013.
- Prepare the servers and install any dependencies, for details see the related tasks link at the end of the topic. During the fix pack installation, an automated prerequisite check tests for completion of these tasks.
- Ensure that you have root access to the IBM Intelligent Operations Center 1.0 event and management server.

**Note:** If you install the IBM Intelligent Operations Center 1.0 Fix Pack 1 before installing the IBM Intelligent Operations Center solution, the heartbeat services for WebSphere MQ and WebSphere Message Broker will not be available.

## Non-English language environment

The IBM Intelligent Operations Center 1.0 Fix Pack 1 can only be installed on a system environment with the English language. If you want to install the fix pack on another language environment, you must first set English as the system language and reset to the other language after installation. Follow these steps to set English as the system language:

1. From the Linux desktop of each server, click **System > Administration > Language**.
2. In the **Language Selection** dialog, select **English(USA)**.
3. Click **OK** to submit the configuration.
4. Log off and log on again.

## Copying the required files and setting parameters

If you have complied with the requirements and prerequisites, download the fix pack. To download the fix pack see the related information link at the end of the topic. You are now ready to copy the files and set the parameters required for installation.

### Related concepts:

“Hardware requirements” on page 12

Each IBM Intelligent Operations Center server and client must meet the recommended hardware requirements.

“Software requirements” on page 14

Each IBM Intelligent Operations Center server and client must meet the minimum software requirements.

“System configuration” on page 9

The IBM Intelligent Operations Center installs and configures an environment with production servers and one server used during the installation process.

### Related tasks:

“Preparing the servers” on page 16

Before you begin the installation, first prepare the servers that the IBM Intelligent Operations Center will be installed on.

“Extracting installation files and installing dependencies” on page 18

After copying the required files to a temporary location, extract the installation files. Then install the dependencies before deploying the IBM Intelligent Operations Center.

“Installing the fix pack” on page 41

Use the command line to install the IBM Intelligent Operations Center 1.0 Fix Pack 1.

### Related information:

 [PO00007 Fix Download](#)

 [PO00013 Fix Download](#)

 [Fix Pack 1 Download](#)

## Copying files required for the fix pack

### Fix Pack 1

Copy to the installation management server the files required to install the IBM Intelligent Operations Center 1.0 Fix Pack 1.

### About this task

The files shown in Table 11 are placed in a single directory, for example, /images.

Table 11. Files required for the IBM Intelligent Operations Center 1.0 Fix Pack 1

File name	Description
fixpack.tar.gz	Fix pack package
IICv1401_Federated_Release_ModelServer_20110711_10_09_07.zip	Model manager capability in IBM Integrated Information Core 1.4.0.1
TSRM_V721_1of2.tar	Tivoli Service Request Manager
TSRM_V721_2of2.tar	Tivoli Service Request Manager
WASND_LinuxIA64_Custom_v61029_ISC7106.tar.gz	WebSphere Application Server 6.1 for Tivoli Service Request Manager
CI0EEEN.tar	Tivoli Composite Application Manager for Application Diagnostics V7.1: agent for HTTP Servers, Linux on x86, English
CZU9MEN.tar.gz	Tivoli Composite Application Manager agent for Lotus Sametime 6.2.4 Fix Pack 1 English Only, Multiplatform

Table 11. Files required for the IBM Intelligent Operations Center 1.0 Fix Pack 1 (continued)

File name	Description
CZ1I3ML.tar	Tivoli Composite Application Manager for Applications Version 6.2.2 Lotus Domino Agent, Multiplatform, Multilingual
CZU9LEN.tar	Tivoli Composite Application Manager agents for WebSphere Messaging 7.0.1 Fix Pack 1: Multiplatform, English
v9.7fp4_linuxx64_server.tar.gz	DB2 Enterprise Server Edition Version 9.7 Fix Pack 4
WASND70013Linux64.tar.gz	WebSphere Application Server Network Deployment 7.0.0.13
7.0.0.19-WS-UPDI-LinuxAMD64.tar.gz	Update Installer for WebSphere Application Server
7.0.0.0-WS-WASJavaSDK-LinuxX64-IFPM32175.pak	WebSphere Application Server 7 JDK Fix Pack
C1G36ML.tar.gz	IBM HTTP Server IBM HTTP Server 7.0
CZAV8EN.tar	IBM Tivoli Monitoring 6.2.2 (WebSphere Application Server Agent)
CZDP7ML.tar	IBM Tivoli Monitoring 6.2.2 (DB2 Agent)
CZ8XZEN.tar.gz	IBM Tivoli Monitoring 6.2.2
7.0.0-WS-WAS-LinuxX64-FP0000019.pak	WebSphere Application Server Fix Pack 7.0.0.19
7.0.0-WS-WASSDK-LinuxX64-FP0000019.pak	WebSphere Application Server 7 JDK Fix Pack 7.0.0.19
7.0.0-WP-Multi-FP002.zip	WebSphere Portal Enable Fix Pack 7.0.0.2
7.0-WP-UpdateInstaller-Linux-x86.tar.gz	WebSphere Portal Enable Update Installer 7.0
6.2.0.3-TIV-ITDS-LinuxX64-IF0002.tar	Tivoli Directory Server Fix Pack 6.2.0.3.2
7.0.1-WS-MQ-LinuxX64-FP0007.tar.gz	WebSphere MQ Fix Pack 7.0.1.7

## Procedure

1. Obtain the IBM Intelligent Operations Center 1.0 Fix Pack 1 download from Fix Central.
2. Create an images directory on the installation management server, for example, /images.
3. Copy the files in the IBM Intelligent Operations Center 1.0 Fix Pack 1 download to the installation management server images directory:
4. Copy the file, v9.7fp4\_linuxx64\_server.tar.gz, from the IBM Intelligent Operations Center 1.0 interim fix PO00002 installation download to the images directory.
5. Copy the following files from the IBM Intelligent Operations Center 1.0 installation media, to the images directory:
  - C1G36ML.tar.gz
  - CZAV8EN.tar
  - CZDP7ML.tar
  - CZ8XZEN.tar.gz
6. Unpack the fixpack.tar.gz file and extract the fix pack installer using the following command: tar -zxvf fixpack.tar.gz.
7. Copy extracted file, images.md5 to the images directory and use the md5sum command to validate images as follows:

```
cp fixpack/images.md5 /images
cd /images
md5sum -c images.md5
```

## What to do next

Set parameters.

### Related tasks:

“Getting fixes from Fix Central” on page 136

You can use Fix Central to find the fixes that are recommended by IBM Support for various products, including IBM Intelligent Operations Center. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. An IBM Intelligent Operations Center product fix might be available to resolve your problem.

“Setting parameters”

When you have copied and extracted the files required for the IBM Intelligent Operations Center 1.0 Fix Pack 1, set the required parameters.

## Setting parameters

Fix Pack 1

When you have copied and extracted the files required for the IBM Intelligent Operations Center 1.0 Fix Pack 1, set the required parameters.

### Procedure

1. Edit the `install.props` file located in the `fixpack/` folder on the installation management server.
2. Provide values for the parameters listed in Table 12.

**Note:** The Tivoli Service Request Manager parameters enable you to select the option of installing the fix pack on top of an existing Tivoli Service Request Manager installation. For the fix pack installation to complete successfully, you must either have an existing Tivoli Service Request Manager installation or set the parameters to install Tivoli Service Request Manager.

Table 12. Parameters that must be set for the installation of the fix pack

Parameter	Value
IOC_IMAGE_LOCATION	Full path name of the images directory.
HOST.MGMT_SERVER.HOSTNAME	Fully-qualified host name of the event and management server. <b>Note:</b> Server names are case sensitive. Do not enter IP address or short host name.
HOST.MGMT_SERVER.PASSWORD	Root password of the event and management server.
IOC_CONTROL.PASSWORD	Password of IOControl.sh command, this password is same as the initial password of the event and management server.
HOST.TSRM_SERVER.HOSTNAME	Fully-qualified host name of the Tivoli Service Request Manager server. <b>Note:</b> Server names are case sensitive. Do not enter IP address or short host name.
HOST.TSRM_SERVER.PASSWORD	Root password of the Tivoli Service Request Manager server.
TSRM.WAS.DMGR.PROFILE_PATH	Deployment manager profile path for Tivoli Service Request Manager installation. Provide the existing path if you have already installed Tivoli Service Request Manager manually.

Table 12. Parameters that must be set for the installation of the fix pack (continued)

Parameter	Value
TSRM.WAS.CUSTOM.PROFILE_PATH	Custom profile path for Tivoli Service Request Manager installation. Provide the existing path if you have already installed Tivoli Service Request Manager manually.
TSRM_INSTALL	Indicator for whether or not to install Tivoli Service Request Manager. Enter New to install, or Ready to skip installation.
TSRM_PORTAL_WEBSEAL_SSO	Indicator for whether or not to configure single sign-on between Tivoli Service Request Manager, WebSphere Portal Server, and Tivoli Access Manager WebSEAL. Enter New to configure, or Ready to skip configuration.
TSRM_JMS	Indicates whether or not to configure Java™ Message Service on WebSphere Application Server for Tivoli Service Request Manager. Enter New to configure, or Ready to skip configuration.
TSRM.WAS.ADMIN_USER	Tivoli Service Request Manager WebSphere Application Server administrative user name.
TSRM.WAS.ADMIN_PASSWORD	Tivoli Service Request Manager WebSphere Application Server administrative user password.
TSRM.DB2.DASADM1.PASSWORD	Password of the DB2 user, dasadm1.
TSRM.DB2.DB2INST1.PASSWORD	Password of the DB2 user, db2inst1.
TSRM.DB2.DB2FENC1.PASSWORD	Password of the DB2 user, db2fenc1.
TSRM.DB2.MAXIMO.PASSWORD	Password of the DB2 user, maximo.
TSRM.IHS.IHSADMIN.PASSWORD	Password of IBM HTTP Server administrative user, ihsadmin.
TSRM.MAXADMIN.PASSWORD	Password of the Tivoli Service Request Manager user, maxadmin. <b>Note:</b> This password must be consistent with the Tivoli Service Request Manager administration password used in the IBM Intelligent Operations Center 1.0 solution.
TSRM.MAXREG.PASSWORD	Password of the Tivoli Service Request Manager user, maxreg.
TSRM.MXINTADM.PASSWORD	Password of the Tivoli Service Request Manager user, mxintadm.
PORTAL.ADMIN_USER	WebSphere Portal Enable administrative user name.
PORTAL.ADMIN_PASSWORD	WebSphere Portal Enable administrative user password.
WAS.ADMIN_USER	WebSphere Application Server administrative user name.
WAS.ADMIN_PASSWORD	WebSphere Application Server administrative user password.

3. If any of the server passwords have changed since the IBM Intelligent Operations Center 1.0 was installed, update the corresponding parameter listed in Table 13.

Table 13. Password parameters for IBM Intelligent Operations Center 1.0 servers

Parameter	Root password of the server
HOST.ACCESS_SERVER.PASSWORD	access server
HOST.PORTAL_SERVER.PASSWORD	portal server



Table 13. Password parameters for IBM Intelligent Operations Center 1.0 servers (continued)

Parameter	Root password of the server
HOST.APP_SERVER.PASSWORD	application and integration server
HOST.DB_SERVER.PASSWORD	database server
HOST.ANALYTIC_SERVER.PASSWORD	analytic server

### Related tasks:

“Copying files required for the fix pack” on page 37

Copy to the installation management server the files required to install the IBM Intelligent Operations Center 1.0 Fix Pack 1.

“Verifying the Tivoli Service Request Manager configuration” on page 45

After you configure Tivoli Service Request Manager for the IBM Intelligent Operations Center 1.0 Fix Pack 1, verify that you synchronized users and groups.

“Configuring Tivoli Service Request Manager for the fix pack” on page 44

When the IBM Intelligent Operations Center 1.0 Fix Pack 1 is installed, synchronize users and groups for Tivoli Service Request Manager.

### Related information:

 Tivoli Provisioning Manager Information Center

## Installing the fix pack

Fix Pack 1

Use the command line to install the IBM Intelligent Operations Center 1.0 Fix Pack 1.

### Before you begin

The fix pack defines a user ID and password during installation. Before starting, determine the user ID and password to be defined for the Tivoli Service Request Manager administrator ID and password.

### About this task

There is an automatic prerequisite check included in the fix pack installation script where the script first checks installation prerequisites. Messages are displayed and output is written to a fix pack log file: `preCheck_Topology_ioc_topo_date.log`. For details of the automatic prerequisite check messages, see the related concept linked at the end of the topic.

### Procedure

1. Log on to the event and management server as root.
2. Run the following command to start all components:  
`/opt/IBM/ISP/mgmt/scripts/IOControl.sh start all password`

Where *password* is the password for the IBM Intelligent Operations Center 1.0 administrator defined when the IBM Intelligent Operations Center 1.0 was installed.

3. On the installation management server, navigate to the temporary directory where you copied the IBM Intelligent Operations Center 1.0 Fix Pack 1 installation files.
4. Navigate to the `fixpack` directory. For example, if you copied the files to the `/images` directory, navigate to `/images/fixpack`.
5. Run the following command to start the fix pack installation:  
`/install.sh encryption key`

The value of *encryption key* is the key used for encryption and this key can be any value you choose. You provide this value the first time you run the `install.sh` script and then provide the same value when you run the `install.sh` script later.

- Any errors detected during the installation are listed. If there is a problem, you have the option to stop; or if there is nothing seriously wrong, continue.

## What to do next

When the installation is completed, log on to the event and management server. Run the following commands to restart all components:

```
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh stop all password
/opt/IBM/ISP/mgmt/scripts/IOCControl.sh start all password
```

Where *password* is the password for the IBM Intelligent Operations Center 1.0 administrator defined when the IBM Intelligent Operations Center 1.0 was installed.

To verify that the installation is successful, see the related task linked at the end of the topic.

If the installation fails, see the related links at the end of the topic for information about messages, troubleshooting, and restarting the installation.

### Related concepts:

“What’s new in the fix pack?” on page 6

The IBM Intelligent Operations Center 1.0 Fix Pack 1 delivers stability improvements, upgrades to components, and system-monitoring infrastructure.

“Preparing to install the fix pack” on page 35

Before installing the IBM Intelligent Operations Center 1.0 Fix Pack 1, understand the system configuration, and ensure that the requirements and prerequisites are met.

“CHK: Installation prerequisite checking messages” on page 132

Use the information in this section to understand and respond to error, warning, and informational messages generated during the installation prerequisite checking process.

“Troubleshooting tips” on page 141

This section contains a list of commonly occurring problems and some troubleshooting tips for each item.

### Related tasks:

“Verifying the solution installation” on page 33

You can verify that the IBM Intelligent Operations Center is correctly installed and configured.

“Restarting a failed installation for the fix pack”

If the IBM Intelligent Operations Center 1.0 Fix Pack 1 installation fails, resolve the issue and check the status of the components installed before restarting the installation.

## Restarting a failed installation for the fix pack

### Fix Pack 1

If the IBM Intelligent Operations Center 1.0 Fix Pack 1 installation fails, resolve the issue and check the status of the components installed before restarting the installation.

### Before you begin

There is an automatic prerequisite check included in the fix pack installation script where the script first checks installation prerequisites. Any errors detected during the installation are displayed and written to a fix pack log file: `preCheck_Topology_ioc_topo_date.log`. See the related concept link at the end of the topic for details of messages. Select the option to stop, if there is a serious problem. Check and resolve the issue before restarting the fix pack installation.

## About this task

If the fix pack installation fails, the status of some middleware components is set to "Uncertain" in the topology model file, `/fixpack/ioc/topology/ioc_topo.xml`. Before you resume the installation, complete the procedure. If the installation of a component fails, remove the partially-installed component. Fix the problem that caused the installation failure. Then rerun fix pack installation, so that the component is fully installed.

## Procedure

1. On the installation management server, navigate to the topology model file, `/ioc/topology/ioc_topo.xml`. The path is within the fix pack folder where fix pack package is extracted.
2. Search the topology model file and find all components with "Uncertain" status. Process each one of these components according to the following steps. An example of the lines identifying such a component is as follows:

```
<component version="7.0.1.7" status="Uncertain" id="mq_fixpack" type="mq_fixpack" package="WMBQ">
<connection id="mqbase" role="mq_base"/>
</component>
```
3. To check the installation status of the component, on the target server where the middleware is being installed, check this file: `/tmp/ioc/script/ioc_topo/component_id/UUID.res`. If the file contains 0, the installation is successful, otherwise the installation failed.
  - a. If the component is installed successfully, complete step 4 before you restart the installation.
  - b. If the component is not installed, before you restart the installation remove the partially installed middleware according to the documentation provided for that component .
4. In the topology model file, search for "Uncertain".
5. Change the status attribute of the successfully installed components from "Uncertain" to "Ready".

## What to do next

Restart the installation by running the same command and encryption key you used previously for installing the fix pack. Then select **resume previous install**. If you change the `install.props` file, start the fix pack installation again by selecting **start new install**.

**Note:** If you select **start new install**, ensure that you have clean servers, prepared as instructed for installing the fix pack, and all components are on.

When resuming an installation, you might receive the errors in the prerequisite check indicating servers are stopped, as follows:

```
CHK014E : Can not connect to WAS profile ISKMgr01 with on server XXX.
CHK022E : WAS server MEMBER01 on profile ISKCustom01 is not started on server XXX.
CHK022E : WAS server MEMBER02 on profile ISKCustom02 is not started on server XXX.
```

To restart the servers, log on to the analytic server as root and run these commands in sequence:

```
/opt/IBM/WebSphere/AppServer/profiles/ISKMgr01/bin/startManager.sh
/opt/IBM/WebSphere/AppServer/profiles/ISKCustom01/bin/startNode.sh
/opt/IBM/WebSphere/AppServer/profiles/ISKCustom01/bin/startServer.sh MEMBER01
/opt/IBM/WebSphere/AppServer/profiles/ISKCustom02/bin/startNode.sh
/opt/IBM/WebSphere/AppServer/profiles/ISKCustom02/bin/startServer.sh MEMBER02
```

### Related concepts:

“CHK: Installation prerequisite checking messages” on page 132

Use the information in this section to understand and respond to error, warning, and informational messages generated during the installation prerequisite checking process.

“Troubleshooting tips” on page 141

This section contains a list of commonly occurring problems and some troubleshooting tips for each item.

### Related tasks:

“Installing the fix pack” on page 41

Use the command line to install the IBM Intelligent Operations Center 1.0 Fix Pack 1.

## Post-installation configuration

### Fix Pack 1

On completion of Tivoli Service Request Manager installation with the IBM Intelligent Operations Center 1.0 Fix Pack 1, additional steps are required to configure Tivoli Service Request Manager.

## Configuring Tivoli Service Request Manager for the fix pack

### Fix Pack 1

When the IBM Intelligent Operations Center 1.0 Fix Pack 1 is installed, synchronize users and groups for Tivoli Service Request Manager.

### About this task

This task is not required if you opted to omit installation of Tivoli Service Request Manager during installation of the fix pack.

### Procedure

1. Open a web browser and link to `http://tsrm.server.hostname:9080/maximo/ui/login`
2. Log on to Tivoli Service Request Manager using the user ID, `maxadmin`.
3. Click **System Configuration > Platform Configuration > Cron Task Setup**.
4. Enter `VMM` in the **Cron Task** field.
5. Click **VMMSYNC**.
6. Configure the **Principal** and **Credential** parameters as follows:

Option	Description
<b>Principal</b>	The value should be <code>uid=admin,o=defaultWIMFileBasedRealm</code> , where <code>admin</code> is the value of <code>TSRM.WAS.ADMIN_USER</code>
<b>Credential</b>	The value should be the password used for the principal account. In this case, enter the value of <code>TSRM.WAS.ADMIN_PASSWORD</code>

For more information about the parameter settings and values required, see the related link at the end of the topic.

7. Select the **Active** check box.
8. Click **Save**.
9. By default, the cron task runs every 5 minutes. Enter a new time in the **Schedule** field of the cron task if you want to change the time interval.

## What to do next

To verify the configuration, see the related task link at the end of the topic.

### Related tasks:

“Verifying the Tivoli Service Request Manager configuration”

After you configure Tivoli Service Request Manager for the IBM Intelligent Operations Center 1.0 Fix Pack 1, verify that you synchronized users and groups.

“Setting parameters” on page 39

When you have copied and extracted the files required for the IBM Intelligent Operations Center 1.0 Fix Pack 1, set the required parameters.

## Verifying the Tivoli Service Request Manager configuration

Fix Pack 1

After you configure Tivoli Service Request Manager for the IBM Intelligent Operations Center 1.0 Fix Pack 1, verify that you synchronized users and groups.

### Procedure

1. Add a user to the IBM Intelligent Operations Center using the portal server administration console.
2. Wait for the next scheduled cron task to run.
3. Open a web browser and link to `http://tsrm.server.hostname:9080/maximo/ui/login`
4. Log on to the Tivoli Service Request Manager using the user ID, maxadmin.
5. Click **Security > Users** and **Enter** to see all the IBM Intelligent Operations Center users added.

### Results

If you can see the IBM Intelligent Operations Center users you added, you verified that the cron task worked.

## What to do next

If you cannot see the IBM Intelligent Operations Center users you added, the cron task does not work. Restart the Tivoli Service Request Manager server and repeat the verification task and the configuration task. Restart the Tivoli Service Request Manager, as follows:

1. Close any browsers connected to `http://tsrm.server.hostname:9080/maximo/ui/login`
2. Log on to the Tivoli Service Request Manager server as root.
3. Stop the Tivoli Service Request Manager using the following commands:  

```
/opt/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/bin/stopServer.sh MXServer  
/opt/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/bin/stopNode.sh  
/opt/IBM/WebSphere/AppServer/profiles/ctgDmgr01/bin/stopManager.sh
```
4. In the dialog box, enter the user ID and password using the values of `TSRM.WAS.ADMIN_USER` and `TSRM.WAS.ADMIN_PASSWORD`. For more information about the parameter settings and values required, see the related task linked at the end of the topic.
5. Start the Tivoli Service Request Manager using the following commands:  

```
/opt/IBM/WebSphere/AppServer/profiles/ctgDmgr01/bin/startManager.sh  
/opt/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/bin/startNode.sh  
/opt/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/bin/startServer.sh MXServer
```

**Related tasks:**

“Setting parameters” on page 39

When you have copied and extracted the files required for the IBM Intelligent Operations Center 1.0 Fix Pack 1, set the required parameters.

“Adding a user or group” on page 52

Select a group and create a user profile to add a new user to the IBM Intelligent Operations Center. Select a group name to add a new group.

“Configuring Tivoli Service Request Manager for the fix pack” on page 44

When the IBM Intelligent Operations Center 1.0 Fix Pack 1 is installed, synchronize users and groups for Tivoli Service Request Manager.

**Related information:**

Tivoli Provisioning Manager Information Center

---

## Chapter 3. Securing the solution

Security is important because the IBM Intelligent Operations Center is central to essential operations. To ensure security, it is important that you manage users of the solution and give all users the correct level of access within the IBM Intelligent Operations Center.

**Note:** Your first task in securing the solution is to ensure that all default passwords have been changed.

User authentication is associated with authorization rights that give the user access to the appropriate features and data. The IBM Intelligent Operations Center supports integration to the existing security infrastructure for single sign-on.

IBM Intelligent Operations Center user permissions are managed through WebSphere Portal users and groups. WebSphere Portal uses the Lightweight Directory Access Protocol (LDAP) database provided by the Tivoli Directory Server running on the event and management server.

The security system provided with the IBM Intelligent Operations Center can accommodate many user groups, roles, and permissions. Accommodating many user groups, roles, and permissions can lead to a security regime that is difficult to manage. It is recommended that administrators restrict the number of groups and permissions.

### User roles and permissions

Membership of a role-based user group provides a way of controlling access to the IBM Intelligent Operations Center. The users in a group have access only to the features of the solution corresponding to their role. Being a member of a role-based user group also helps users to focus on the appropriate tasks. The standard roles are: Executive, Supervisor, and Operator.

To add a user to the IBM Intelligent Operations Center:

1. Choose a group appropriate to the role of the user in the organization and make the user a member of that group.
2. Complete a profile for the user including at least the user ID, name, and password.

### Data categories and permissions

The security of data that is stored in databases in the IBM Intelligent Operations Center is managed by implementing role-based access to the databases. Access to a feature of the IBM Intelligent Operations Center does not mean that all data is available to the user. Data security is applied at the server level to ensure that users see only the appropriate data. The standard categories are : Geophysical, Transportation, Meteorological, Environmental, Infrastructure, Chemical, Biological, Safety, Security, Rescue, Fire, Health, and Other.

### WebSphere Portal

WebSphere Portal is a component of the IBM Intelligent Operations Center solution. It provides a platform that can be scaled to accommodate the required set of users. It also provides role-based access that can be adjusted to reflect the required organization structure. The documentation set for the IBM WebSphere Portal is not included in the solution. Instead the IBM Intelligent Operations Center documentation points to the documentation for WebSphere Portal where relevant. You can view, create, and delete users or user groups with the **Manage Users and Groups** portlet. You can also change group memberships. A link is provided at the end of this topic to the WebSphere Portal documentation on this portlet.

## Related information:

 [IBM WebSphere Portal documentation](#)

## User roles and access

The IBM Intelligent Operations Center implements security by limiting access to features based on user roles.

To use a specific feature of the IBM Intelligent Operations Center, a user must be a member of the user role group that provides the required access to that feature. A user is made a member of a user role group by an administrator. The following table shows how real-life roles might map to the user role groups with login access levels in the IBM Intelligent Operations Center.

*Table 14. Job roles and IBM Intelligent Operations Center user role groups*

Job Role	Responsibilities	User role group
Executive	<ul style="list-style-type: none"><li>• Defines event, incident, and key performance indicator (KPI) input requirements and thresholds</li><li>• Views high level visual summaries, details, and reports of:<ul style="list-style-type: none"><li>– KPIs</li><li>– Events</li></ul></li><li>• Communicates policy, long-term direction, or high-level decisions</li></ul>	City-wide Executive
Supervisor or manager	<ul style="list-style-type: none"><li>• Manages events and incidents</li><li>• Produces and monitors KPI reports</li><li>• Issues alerts</li><li>• Analyzes events for change of status or action requirements</li><li>• Decides on short-term corrective measures</li></ul>	City-wide Supervisor
Operator	<ul style="list-style-type: none"><li>• Monitors event information</li><li>• Monitors alerts</li><li>• Views details</li><li>• Issues communications</li><li>• Updates event or incident data with further information, for example:<ul style="list-style-type: none"><li>– Telephone reports</li><li>– Inputs from construction or maintenance</li></ul></li></ul>	City-wide Operator
User Administrator	Administers all aspects of users including defining groups, assigning permissions to groups, and assigning users to groups. Provides users with the correct access level. Access level is assigned based on group membership.	wpsadmins

Before customizing roles and defining users for your organization, familiarize yourself with the IBM Intelligent Operations Center security system.



**Related tasks:**

“Adding a user or group” on page 52

Select a group and create a user profile to add a new user to the IBM Intelligent Operations Center. Select a group name to add a new group.

**Related reference:**

“User role groups and authorization permissions”

A set of permissions for accessing features in the IBM Intelligent Operations Center is associated with each user role group.

“User category groups and data permissions” on page 51

Permission to access a category of data in the IBM Intelligent Operations Center is associated with each user category group.

## Sample users

During the deployment of the IBM Intelligent Operations Center, sample users are created.

Generic sample users are defined with user role groups and corresponding access permissions. Some are defined as examples, but others are required for administration of the solution, as shown in the following table.

*Table 15. Sample users defined in the IBM Intelligent Operations Center*

User ID	User role group
<b>Required user</b>	
wpsadmin	wpsadmins
<b>Example users</b>	
tdelorne	City-wide Executive
scollins	City-wide Supervisor
akelly	City-wide Operator

When you are ready to define users for your organization, delete the example users. You must not delete a required user. Required users are essential for administration tasks associated with the IBM Intelligent Operations Center.

**Important:** For the required user, replace the default password by assigning a new password. For information on updating user IDs and passwords, see the WebSphere Portal documentation.

**Related tasks:**

“Deleting sample users” on page 33

The IBM Intelligent Operations Center is shipped with sample users. For security reasons these users should be deleted after the IBM Intelligent Operations Center is installed.

**Related information:**

 [WebSphere Portal Information Center](#)

## User role groups and authorization permissions

A set of permissions for accessing features in the IBM Intelligent Operations Center is associated with each user role group.

An administrator assigns a role to a user by making the user a member of the corresponding user role group. Each user is assigned membership of one or more user role groups.

The following table lists the permissions for each user role group supplied with the IBM Intelligent Operations Center. For each user role group, an authorization permission is granted for each feature in the IBM Intelligent Operations Center.

*Table 16. IBM Intelligent Operations Center features and associated user role group permissions*

Feature type	Feature name	City-wide Executive	City-wide Supervisor	City-wide Operator	wpsadmins
Portal	User and Groups	None	None	None	Administrator permission
Page	Executive	User permission	User permission	None	Administrator permission
Portlet	Status	User permission	User permission	None	Administrator permission
Portlet	Key Performance Indicator Drill Down	User permission	User permission	None	Administrator permission
Portlet	Coordinator - Alerts	User permission	User permission	User permission	Administrator permission
Portlet	Contacts	User permission	User permission	User permission	Administrator permission
Portlet	Operations	None	User permission	User permission	Administrator permission
Portlet	Map	None	User permission	User permission	Administrator permission
Page	Events	None	User permission	User permission	Administrator permission
Portlet	Security	None	None	None	Administrator permission
Portlet	Sample Publisher	None	None	None	Administrator permission
Portlet	Intelligent Operations Center - About	None	None	None	Administrator permission

The IBM Intelligent Operations Center authorization permissions are assigned based on Lightweight Directory Access Protocol (LDAP) groups. The permissions are defined as follows:

- User permission is the authority granted to a user to give them access to view and work with features.
- Administrator permission is the authority granted to an administrator to give them access to:
  - configure features
  - create, modify or delete users and user groups

To access data in IBM Intelligent Operations Center a user must be a member of the user category group that provides the required data permissions.

**Related concepts:**

“Security” on page 56

Use the Security portlet to view the permissions associated with the IBM Intelligent Operations Center users and groups.

“User roles and access” on page 48

The IBM Intelligent Operations Center implements security by limiting access to features based on user roles.

**Related tasks:**

“Adding a user or group” on page 52

Select a group and create a user profile to add a new user to the IBM Intelligent Operations Center. Select a group name to add a new group.

“Viewing or modifying group membership” on page 53

View or modify group membership to manage the access permissions of users within the IBM Intelligent Operations Center.

**Related reference:**

“User category groups and data permissions”

Permission to access a category of data in the IBM Intelligent Operations Center is associated with each user category group.

**Related information:**

 [IBM WebSphere Portal documentation](#)

## User category groups and data permissions

Permission to access a category of data in the IBM Intelligent Operations Center is associated with each user category group.

An administrator assigns data access to a user by making the user a member of the appropriate user category group. Each user is assigned membership of one or more user category groups.

The following table lists the data categories covered by the IBM Intelligent Operations Center and the corresponding user category groups used to identify event, key performance indicator (KPIs), and alert data. For example, if a user wants to be able to see events related to the city’s water department, the user must be a member of the group `ioc_base_infrastructure`.

*Table 17. User category group descriptions and identifiers*

Data category	Description	User category group
CBRNE	Chemical, biological, radiological, nuclear, or high-yield explosive threat or attack	<code>ioc_base_chemical</code> , <code>ioc_base_biological</code> , <code>ioc_base_radiological</code> , <code>ioc_base_nuclear</code> , <code>ioc_base_explosive</code>
Env	Environment: pollution and other environmental	<code>ioc_base_environmental</code>
Fire	Fire suppression and rescue	<code>ioc_base_fire</code>
Geo	Geophysical (including landslide)	<code>ioc_base_geophysical</code>
Health	Medical and public health	<code>ioc_base_health</code>
Infra	Infrastructure: utility, telecommunication, other non-transport infrastructure	<code>ioc_base_infrastructure</code>
Met	Meteorological (including flood)	<code>ioc_base_meteorological</code>
Rescue	Rescue and recovery	<code>ioc_base_rescue</code>
Safety	General emergency and public safety	<code>ioc_base_safety</code>
Security	Law enforcement, military, homeland, and local/private security	<code>ioc_base_security</code>

Table 17. User category group descriptions and identifiers (continued)

Data category	Description	User category group
Transport	Public and private transportation	ioc_base_transportation
Other	Other events, KPIs, or alerts	ioc_base_other

To login and access features of the IBM Intelligent Operations Center, a user must be a member of the user role group that provides the required authorization permissions.

**Related concepts:**

“Security” on page 56

Use the Security portlet to view the permissions associated with the IBM Intelligent Operations Center users and groups.

“User roles and access” on page 48

The IBM Intelligent Operations Center implements security by limiting access to features based on user roles.

**Related tasks:**

“Adding a user or group”

Select a group and create a user profile to add a new user to the IBM Intelligent Operations Center. Select a group name to add a new group.

“Viewing or modifying group membership” on page 53

View or modify group membership to manage the access permissions of users within the IBM Intelligent Operations Center.

**Related reference:**

“User role groups and authorization permissions” on page 49

A set of permissions for accessing features in the IBM Intelligent Operations Center is associated with each user role group.

**Related information:**

 [IBM WebSphere Portal documentation](#)

## Adding a user or group

Select a group and create a user profile to add a new user to the IBM Intelligent Operations Center. Select a group name to add a new group.

### About this task

First select a user role group to set the correct level of access permissions when adding a new user. Then complete the fields on the **Profile Management** page so that the IBM Intelligent Operations Center has the required information to add the new user. Follow the link at the end of the topic for more information about what you can enter in the fields on the **Profile Management** page.

### Procedure

1. Log on to `http://portalServer/wps/myportal` as an administrative user.
2. Click **Administration** on the navigation bar at the top of the page.
3. Click **Access** on the sidebar menu.
4. Click **Users and Groups** on the submenu.
5. If you are adding a new user, select a role by giving the user membership of a group. Search for the group by clicking **All Portal User Groups** for a list of groups and click the required group.
6. Click **New User** or **New Group**.
7. If you are creating a user group, enter a name for the user group.

8. If you are adding a new user, ensure that you enter all of the required fields in the user profile as indicated by the asterisks.
9. Click **OK** to submit the new profile or group.

## Results

A message confirms if the submission is successful. A new user profile is created and displayed on the group list or a new group is displayed. The new user is authorized to access the IBM Intelligent Operations Center according to the permissions assigned to the role group selected.

## What to do next

- Give the new user membership of data category groups according to the data permissions required.
- If a new group has been added, add the group to the WebSphere Application Server Network Deployment junction ACL.
- If a new group has been added, authorization permissions must also be set for the group. The authorization permissions define what features and data members of the group can see and modify. For information on setting authorization permissions, see the IBM WebSphere Portal 7 Product Documentation and search for information on assigning access to pages.

**Note:** To save time you can duplicate group assignments for a new user based on an existing user. Select the new user and click the **Duplicate** icon. Select the existing user to duplicate group membership.

### Related concepts:

“User roles and access” on page 48

The IBM Intelligent Operations Center implements security by limiting access to features based on user roles.

### Related tasks:

“Verifying the Tivoli Service Request Manager configuration” on page 45

After you configure Tivoli Service Request Manager for the IBM Intelligent Operations Center 1.0 Fix Pack 1, verify that you synchronized users and groups.

“Managing a Tivoli Access Manager WebSEAL junction ACL using the command line” on page 57

To add a new user or group to the Tivoli Access Manager WebSEAL junction ACL, run a series of commands.

“Managing a Tivoli Access Manager WebSEAL junction ACL using the Tivoli Access Manager WebSEAL Web Portal Manager” on page 57

To add new users or groups to the Tivoli Access Manager WebSEAL junction ACL, use the Tivoli Access Manager WebSEAL Web Portal Manager.

### Related reference:

“User role groups and authorization permissions” on page 49

A set of permissions for accessing features in the IBM Intelligent Operations Center is associated with each user role group.

“User category groups and data permissions” on page 51

Permission to access a category of data in the IBM Intelligent Operations Center is associated with each user category group.

### Related information:

 [IBM WebSphere Portal documentation](#)

---

## Viewing or modifying group membership

View or modify group membership to manage the access permissions of users within the IBM Intelligent Operations Center.

## About this task

Select the group corresponding to the role or data category for which you want to view or change membership. Membership of a role group gives users access to the parts of the solution appropriate to that role. Membership of a category group gives users access to the events, key performance indicators (KPIs), and alerts associated with that category.

Hover over an icon to view hover help indicating the purpose of the icon.

## Procedure

1. Log on to `http://portalServer/wps/myportal` as an administrative user.
2. Click **Administration** on the navigation bar at the top of the page.
3. Click **Access** on the sidebar menu.
4. Click **Users and Groups** from the submenu.
5. Click **All Portal User Groups** for a list of groups and click the group you require. The members of the group are listed.
6. You can perform the following actions in relation to group membership:
  - View membership of other groups by clicking **View membership** for the user ID.
  - Add a user or users to the group by clicking **Add member** and selecting the user or users to be added.
  - Remove a user from the group by clicking **Remove** for the user ID.

### Related concepts:

“Security” on page 56

Use the Security portlet to view the permissions associated with the IBM Intelligent Operations Center users and groups.

### Related reference:

“User role groups and authorization permissions” on page 49

A set of permissions for accessing features in the IBM Intelligent Operations Center is associated with each user role group.

“User category groups and data permissions” on page 51

Permission to access a category of data in the IBM Intelligent Operations Center is associated with each user category group.

### Related information:

 [IBM WebSphere Portal documentation](#)

---

## Viewing or editing a user profile

View or edit the profile of a user to set or reset any of the user profile attributes including password. You cannot change the user ID.

## About this task

Select the user from the authenticated portal users list to open the user profile and change profile details. Each user can also change their own profile.

Hover over an icon to view hover help indicating the purpose of the icon.

## Procedure

1. Log on to `http://portalServer/wps/myportal` as an administrative user.
2. Click **Administration** from the top navigation bar.

3. Click **Access** item on the sidebar menu.
4. Click **Users and Groups** from the submenu.
5. Click **All Authenticated Portal Users** for a list of users.
6. Click the edit icon for the user to display the **Profile Management** page. The attribute fields for the user profile are displayed.
7. If you want to change the password, enter a new password in the **New Password:** and **Confirm Password:** fields.
8. You can enter, edit, or delete information in any of the remaining fields.
9. Click **OK** to submit the changes you have made.

## Results

The user profile is updated with the changes you submitted.

### Related information:

 [IBM WebSphere Portal documentation](#)

---

## Deleting a user or group

Delete a user or group from the IBM Intelligent Operations Center.

### About this task

To delete a user, select the user from the list of authenticated portal users and delete. To delete a group, select the group from the list of portal user groups and delete.

Hover over an icon to view hover help indicating the purpose of the icon.

**Note:** Be aware that deleting a user from the IBM Intelligent Operations Center also removes their access to other solutions within the IBM Smarter Cities™ Software Solutions product family. Deleting a group also removes that group from other solutions.

### Procedure

1. Log on to `http://portalServer/wps/myportal` as an administrative user.
2. Click **Administration** on the top navigation bar.
3. Click **Access** on the sidebar menu.
4. Click **Users and Groups** on the submenu:
  - Click **All Portal User Groups** to display a list of groups.
  - Click **All Authenticated Portal Users** to display a list of users.
5. Click the **Delete** icon corresponding to the user or group that you want to delete.

## Results

The user or group that you delete no longer exists in the IBM Intelligent Operations Center. Deleting a group does not delete members of the group.

## Related information:

 [IBM WebSphere Portal documentation](#)

---

## Security

Use the Security portlet to view the permissions associated with the IBM Intelligent Operations Center users and groups.

### What is the Security portlet?

The Security portlet is provided as an administrative and test tool that displays details of group membership and permissions that have been granted to users.

### What does the Security portlet display?

Use the **User** tab to check permissions for a user. Enter the user ID to view the following information:

- A complete list of all the data categories and user category groups available in the IBM Intelligent Operations Center.
- A list of the data category permissions assigned to the specified user.
- A list of all the groups, user role groups and user category groups, of which the specified user is a member.
- A list of each data category indicating if the specified user has been granted permission for that category.

Use the **Summary** tab to check summary statistics for users and group permissions. You can view the following information:

- Total number of groups in the IBM Intelligent Operations Center.
- Total number of users authorized to access the IBM Intelligent Operations Center.
- A list of the total number of users by data category.
- A list of the total number of users by user role group.

For more information about user permissions, go to the IBM Intelligent Operations Center Information Center and search for securing the solution.

#### Related tasks:

“Viewing or modifying group membership” on page 53

View or modify group membership to manage the access permissions of users within the IBM Intelligent Operations Center.

#### Related reference:

“User role groups and authorization permissions” on page 49

A set of permissions for accessing features in the IBM Intelligent Operations Center is associated with each user role group.

“User category groups and data permissions” on page 51

Permission to access a category of data in the IBM Intelligent Operations Center is associated with each user category group.

---

## Managing a Tivoli Access Manager WebSEAL junction ACL

To manage users and groups defined in the Tivoli Access Manager WebSEAL junction, an administrator can use commands or the Tivoli Access Manager Web Portal Manager.

New groups added to the Tivoli Access Manager WebSEAL junction ACL need to be added to the IBM Intelligent Operations Center as well.



### Related concepts:

“Creating a WebSphere Application Server Network Deployment junction” on page 30

You can deploy an application on the WebSphere Application Server Network Deployment. This is an optional task. To complete the task, you must create a junction and ACL for the WebSphere Application Server Network Deployment. To do this, use either a command line or the Tivoli Access Manager Web Portal Manager.

## Managing a Tivoli Access Manager WebSEAL junction ACL using the command line

To add a new user or group to the Tivoli Access Manager WebSEAL junction ACL, run a series of commands.

### Procedure

1. On the access server, log in to the Tivoli Access Manager WebSEAL server terminal using the following commands:

```
# pdadmin
login
```

2. Enter `sec_master` for the user ID and enter the password.
3. To show the properties of the ACL, run the following command:  
`object show /WebSEAL/WebSeal_hostname-WebSEAL_instance_name/ACL_name`
4. Complete the appropriate substep.

- To add a user:

```
acl modify ACL_name set user user_name Tdrx
```

- To add a group:

```
acl modify ACL_name set group group_name Tdrx
```

### Related tasks:

“Adding a user or group” on page 52

Select a group and create a user profile to add a new user to the IBM Intelligent Operations Center. Select a group name to add a new group.

## Managing a Tivoli Access Manager WebSEAL junction ACL using the Tivoli Access Manager WebSEAL Web Portal Manager

To add new users or groups to the Tivoli Access Manager WebSEAL junction ACL, use the Tivoli Access Manager WebSEAL Web Portal Manager.

### Procedure

1. Access the Tivoli Access Manager WebSEAL Web Portal Manager at the following URL:

```
http://events_and_mangement_server_hostname:9061/ibm/console
```

Enter the administrator user ID and password created when the IBM Intelligent Operations Center was installed.

2. Click **Tivoli Access Manager > Web Portal Manager > ACL > List ACL**.

Enter `sec_master` for the user ID and enter the password.

3. Select the ACL you want to change.
4. Click **Create**.
5. To create a new user, complete the following substeps:
  - a. Change **Entry Type** to **User**.
  - b. Enter the new user name in **Entry Name**.
  - c. Select the following permissions: **Traverse**, **Delete**, **Read**, and **Execute**.
  - d. Click **Apply**.

To create a new group, complete the following substeps:

- a. Change **Entry Type** to Group.
- b. Enter the new group name in **Entry Name**.
- c. Select the following permissions: **Traverse**, **Delete**, **Read**, and **Execute**.
- d. Click **Apply**.

## Results

The new user or group is added to the ACL.

### Related tasks:

“Adding a user or group” on page 52

Select a group and create a user profile to add a new user to the IBM Intelligent Operations Center. Select a group name to add a new group.

---

## Importing users and groups

You can import users from an existing external Lightweight Directory Access Protocol (LDAP) directory. Use the middleware directory management products that are provided with the IBM Intelligent Operations Center and base architecture.

There are several ways to import users and groups into the IBM Intelligent Operations Center. Here are two possible methods:

### Using an LDIF file to import users and groups into the Tivoli Directory Server

An LDAP administrator must perform the following procedure on the IBM Intelligent Operations Center event and management server.

1. Import the LDAP Directory Interchange Format (LDIF) file into the Tivoli Directory Server.
2. Import the users and groups into Tivoli Access Manager WebSEAL.
3. Set the following Tivoli Access Manager WebSEAL user account attributes by using the user modify commands:
  - `account-valid {yes}`
  - `password-valid {yes}`

### Using the Portal server admin console GUI

The Portal administrator, for example, `wpsadmin`, must perform the following procedure on the IBM Intelligent Operations Center portal server. The administrator can use either the admin console or run a WebSphere Portal Server `CreateUser.xml` script to import and manage users and groups. The WebSphere Portal Server automatically creates the associated entries in Tivoli Access Manager WebSEAL and in the directory on the Tivoli Directory Server.

### Related information:

 [Tivoli Directory Server Information Center](#)

 [Tivoli Access Manager Information Center](#)

 [WebSphere Portal Information Center](#)

---

## Chapter 4. Integrating the solution

Products and services can be integrated with the IBM Intelligent Operations Center using events.

Events communicated to the IBM Intelligent Operations Center must be in the Common Alerting Protocol. These events can relate to key performance indicators (KPI) monitored by the IBM Intelligent Operations Center or might be unrelated to KPIs.

---

### Examples of systems that can be integrated

Products and services can be integrated with the IBM Intelligent Operations Center.

Examples of systems and services include:

- Systems reporting on public safety issues.
- Systems reporting on traffic events.
- Systems reporting on water quality and usage.
- Systems providing data on outages and status of related work orders.

These systems must be able to communicate with the IBM Intelligent Operations Center and send events and measurements in the supported protocol to the IBM Intelligent Operations Center inbound event queue.

#### Related concepts:

“Using the inbound event queue defined for the IBM Intelligent Operations Center” on page 68  
CAP events can be published into the IBM Intelligent Operations Center by directing them to the included WebSphere Message Broker instance.

“Integrating with the Common Alerting Protocol” on page 61

The Common Alerting Protocol (CAP) is used to exchange event information between the IBM Intelligent Operations Center and external systems.

---

### Integration points and protocols

Products and services can be integrated with the IBM Intelligent Operations Center through the WebSphere Message Broker. Processing definitions for key performance indicators (KPIs) are created using Rational Application Developer and the IBM WebSphere Business Monitor Developers toolkit. KPIs are monitored by IBM WebSphere Business Monitor.

### Events and KPIs

The IBM Intelligent Operations Center uses events and key performance indicators (KPIs) to determine how information is displayed.

Events are received by the IBM Intelligent Operations Center. These events can be displayed on the Events portlet and can affect the display of the Map portlet.

KPI definitions determine how events will be displayed. For example, if a KPI threshold is exceeded, the event might be flagged with a higher urgency or severity. Events without corresponding KPI definitions will be displayed with the information received.

KPI definitions also determine the status portlet display.

Events must be received by IBM Intelligent Operations Center in the Common Alerting Protocol (CAP) format. The processing of KPIs is defined using Rational Application Developer with the IBM WebSphere Business Monitor toolkit installed.

**Related concepts:**

“Executive view” on page 108

Use the Executive view to obtain a consolidated view of key performance indicators (KPIs) and alerts associated with the KPIs. The Executive view enables users with cross-organization responsibility to monitor, manage, and respond to status changes in relation to the key areas of organizational performance and well-being.

“Operations view” on page 113

Use the Operations view to maintain awareness of events. It is intended for operators, managers, or others monitoring current events and planning future events.

“Customizing KPIs” on page 72

Key performance indicators (KPIs) can be created and modified using the IBM WebSphere Business Monitor and the IBM WebSphere Business Monitor Development Toolkit.

**Policy for KPI updates**

The IBM Intelligent Operations Center policy determines if an incoming event is a KPI event update, then sends it for processing to generate a KPI update or an alert depending on parameters. A KPI event is determined by `<code>KPI</code>` in the alert block of the Common Alerting Protocol XML.

If the event is confirmed as a KPI update, the policy checks the KPI parameters and generates a KPI event XML to send to the IBM WebSphere Business Monitor for processing.

The following table shows a sample KPI event update.

*Table 18. Sample KPI event properties*

Property	Value
Sender	security@rtp.city.gov
Event type	Crime Response Time
Event status	Actual- actionable by all target recipients
Event scope	Public - For general dissemination to unrestricted audiences
Category	Security
Severity	Severe
Certainty	Likely
Urgency	Immediate
Message type	Alert- initial information requiring attention by targeted recipients
Description	Burglary
Sent date / time	2011-04-18T02:28:10-05:00

The following table shows the sample KPI parameters associated with the KPI event update in Table 18.

*Table 19. Sample KPI event parameters*

Parameter	Value
Report Number	1111
Precinct	Precinct One
Responded	2011-02-15T15:05:07-05:00

**Related concepts:**

“Status” on page 109

Use the Status portlet to see the status of key performance indicators (KPIs) for a single organization or across organizations.

“Coordinator - Alerts” on page 111

Use the Coordinator - Alerts portlet to view your alert messages and their details.

**Policy for event correlation**

The event correlation policy determines if the IBM Intelligent Operations Center identifies events affecting one another due to their time or proximity.

Event correlation depends on the timeframe and location within which events occur, defined as follows:

- The timeframe of an event is defined by the values of the onset date and time, and the values of the expired date and time for the event. The default timeframe for event correlation is set to within two hours.
- The location of an event is defined by the latitude and longitude coordinates, and the radius of the circle of an area associated with the event. Not all events are associated with an area and a radius, the default value is 0. The default distance for event correlation is set to within 5 miles.

If an incoming event meets both of the correlation criteria, an alert will be generated in the Coordinator - Alerts portlet. It is possible for two or more events to meet the correlation criteria. Event correlation criteria can be configured in the IBM Intelligent Operations Center SYSPROP table. The distance, timeframe, and unit of distance can be specified.

**Related concepts:**

“Coordinator - Alerts” on page 111

Use the Coordinator - Alerts portlet to view your alert messages and their details.

“Specifying system-wide configuration data” on page 91

The IBM Intelligent Operations Center SYSPROP table stores IBM Intelligent Operations Center configuration data.

**Integrating with the Common Alerting Protocol**

The Common Alerting Protocol (CAP) is used to exchange event information between the IBM Intelligent Operations Center and external systems.

The CAP is a generic format for exchanging emergency alerts and public warnings over various networks. It provides an open, non-proprietary digital message format for all types of alerts and notifications. The CAP is compatible with emerging techniques, such as web services, while offering enhanced capabilities. These capabilities include:

- Flexible geographic targeting using latitude and longitude shapes and other geospatial representations in three dimensions
- Multilingual and multi-audience messaging
- Phased and delayed effective times and expirations
- Enhanced message update and cancellation features
- Template support for framing complete and effective warning messages
- Digital encryption and signature compatibility
- Digital images and audio facilities

Events are self-contained data messages that can be sent or consumed by all components. Events can be published to topic queues and read by all potentially interested subscribing IT systems. The CAP helps standardize event content so multiple domains can send and receive events in a common format using common conventions. The standard defines the mandatory and optional fields in the event record and the

acceptable values for those fields. Event processing management can mediate between legacy formats and the standardized format. The CAP can be extended to handle day-to-day operations in addition to emergency situations.

Minimally, events must contain:

- A unique event identifier that contains:
  - The sender (system or human)
  - Organization sending the event
  - Serial number within sending system
  - Timestamp of event creation
- Information that allows recipients to define and prioritize responses:
  - Urgency – how rapidly recipients should respond to the alert
  - The level of threat to life and property
  - Certainty – a probability ranging from 100%, the event has been observed, to 0%, the event is now not expected to occur
  - Predicted time for events that might happen in the future
  - Duration of events that have been previously reported and whose continuation is being reported
  - Anticipated duration of events that represent a situation that cannot be corrected promptly
  - Recommended or mandated actions and directives
- Information to allow the event to be correlated:
  - City semantic model references (if one exists)
  - Geospatial coordinates
  - Reference to prerequisite event, or an event that was the precipitating cause
  - Unique asset identifiers for any involved
- Human readable textual descriptions:
  - Location description
  - Activity description

Using the CAP helps minimize per-event data exchange. Because events are formatted in XML, the data format can be written and read by a variety of systems thereby preventing the exchange of meaningless data or data creating dangerous confusion.

The IBM Intelligent Operations Center provides persistent storage of CAP alerts and a standard interface for presenting them.

While the entire CAP structure is accepted by the IBM Intelligent Operations Center, only some data is used by the IBM Intelligent Operations Center when calculating key performance indicators (KPI).

The IBM Intelligent Operations Center uses the WebSphere Message Broker to integrate events using the CAP.

The IBM Intelligent Operations Center supports OASIS Common Alerting Protocol Version 1.2.

### Related concepts:

“Using CAP for KPI events” on page 65

The WebSphere Message Broker, which is provided as part of the IBM Intelligent Operations Center, accepts CAP event messages and uses the data in key performance indicator (KPI) calculations.

“Using CAP for non-KPI events” on page 68

CAP data can also be used to provide data on events not associated with KPI calculations.

“Configuring the IBM Intelligent Operations Center to receive events” on page 68

External event queue messages are received by the IBM Intelligent Operations Center on an inbound queue. The messages must follow the Common Alerting protocol.

### Related information:

 [OASIS Common Alerting Protocol Version 1.2](#)

## CAP structure

Each CAP alert message consists of an `<alert>` segment that can contain one or more `<info>` segments. Each `<info>` segment can include one or more `<area>` segments. In most cases, CAP messages with a `<msgType>` with a value of *alert* includes at least one `<info>` element.

The following are the main message elements.

- `<alert>`

The `<alert>` segment provides basic information about the current message: its purpose, its source, and its status. It also has a unique identifier for the message and links to any other related messages. An `<alert>` segment can be used alone for message acknowledgments, cancellations, or other system functions; however, most alert segments include at least one `<info>` segment.

- `<info>`

The `<info>` segment describes an anticipated or actual event in terms of urgency (the time available to prepare), severity (the intensity of the impact) and certainty (confidence in the observation or prediction). It also provides both categorical and textual descriptions of the subject event. The `<info>` segment might also provide instructions for appropriate response by message recipients and other details, for example hazard duration, technical parameters, contact information, and links to additional information sources. Multiple `<info>` segments can be used to describe differing parameters, such as different probability or intensity bands, or to provide the information in multiple languages.

- `<resource>`

The `<resource>` segment provides an optional reference to additional information related to the `<info>` segment. It might reference a digital asset such as an image or audio file.

- `<area>`

The `<area>` segment describes a geographic area to which the `<info>` segment applies. Textual and coded descriptions (such as postal codes) are supported, but the preferred representations use geospatial shapes, polygons and circles, and an altitude or altitude range expressed in standard latitude, longitude, and altitude terms in accordance with a specified geospatial datum.

### Related concepts:

“Using CAP for KPI events” on page 65

The WebSphere Message Broker, which is provided as part of the IBM Intelligent Operations Center, accepts CAP event messages and uses the data in key performance indicator (KPI) calculations.

“Using CAP for non-KPI events” on page 68

CAP data can also be used to provide data on events not associated with KPI calculations.

## Event types

Several CAP event types are supported by the IBM Intelligent Operations Center.

## Actual/predicted event

These messages are unsolicited messages sent by various domains about abnormal conditions or exceptions. These messages also cover key performance indicator (KPI) violations where an event is created.

## Acknowledgement

An acknowledgement is a CAP message with the following field values in the <alert> element:

- The <msgType> value is set to **ACK** which means the sender acknowledged the receipt and acceptance of the messages identified in <references>.
- The <references> field contains the extended message identifiers (in the format sender, identifier, sent) of an earlier CAP message or messages referenced by the acknowledgement.

•

**Note:** The <info> element is optional for an acknowledgement.

## Advisory

An advisory is a CAP message with the following field values in the <alert> element:

- The <msgType> value is **Alert**.
- The <note> value is **Advisory**.
- The <references> element must contain the identifiers of the CAP message that is the parent (the root cause) of the event.

For example when the water company receives a **Heavy Rainfall** forecast from the weather bureau, the water company publishes a **Water Overflow Advisory** to all other domains. In this case, **Heavy Rainfall** is the parent of the **Water Overflow Advisory**.

## Response

A response is a CAP message with the following field values in the <alert> element:

- The <msgType> value is **Alert**.
- The <note> value is **Response**.
- The <references> element must contain the identifiers of the CAP message to which this is a response

For example, when a city operator sends a **City Brownout Advisory** to various domains, those domains send back a response to the advisory after performing an impact analysis on their individual functions.

## Directive

A directive is the same as an advisory except that the <info> element includes an <eventCode> which includes information about the actions to be performed by a remote domain.

The directive is a CAP message with the following field values in the <alert> element:

- The <msgType> value is **Alert**.
- The <note> value is **Directive**.
- The <references> element must contain the identifiers of the CAP message that is the parent (the root cause) of this event. This field is optional. If a value is specified, it determines the relationship between the events and the directives issued that correspond to those events.
- The <instruction> element is mandatory for directives. It must contain a recommended, requested, or mandatory action to be taken by the recipient of the directive.



## Incident

Incidents are used to collate multiple messages referring to different aspects of the same incident. Incident CAP messages act as a container of all the events that are related to an specific incident. These events can be in different domains.

An advisory is promoted to an incident when domains send back responses to the advisory indicating multi-domain impacts requiring a coordinated action. The <incident> element in all related events is populated with the <identifier> value of the incident event. Related events are events where the <references> value is the same as the <identifier> value of the incident event.

Incident is a CAP message with the following field values in <alert>:

- The <msgType> value is **Alert**.
- The <note> value is **Incident**.
- The <references> element must contain the identifiers of the CAP message that is the parent (the root cause) of this event
- The <incidents> element must contain its own identifier

## Update

An update is a CAP message with following field values in the <alert> element:

- The <msgType> element is set to **update** which means that this update supersedes the earlier messages identified in the <references> element.
- The <references> element contains the extended message identifiers (in the format sender, identifier, sent) of an earlier CAP message or messages referenced by the update.

## Cancel

A cancel is a CAP message with the following field values in the <alert> element:

- The <msgType> element is set to **Cancel** which means that this message cancels the earlier messages identified in the <references> element.
- The <references> element contains the extended message identifiers (in the format sender, identifier, sent) of an earlier CAP message or messages referenced by this cancelation.
- The <note> element contains an explanation of why or how this alert is cleared.

## Close

A close is a CAP message with the following field values in the <alert> element:

- The <msgType> element is set to **Update**.
- The <note> element is set to **Close**.
- The <references> element contains the extended message identifiers (in the format sender, identifier, sent) of an earlier CAP message or messages to be closed.

### Related information:



OASIS Common Alerting Protocol Version 1.2

## Using CAP for KPI events

The WebSphere Message Broker, which is provided as part of the IBM Intelligent Operations Center, accepts CAP event messages and uses the data in key performance indicator (KPI) calculations.

Table 20 on page 66 lists the data elements used in KPI calculations:

Table 20. CAP elements used in IBM Intelligent Operations Center KPI calculations

Required or Optional	Data Element (normative)	Description
Required	Message_ID (identifier)	Unique message identifier
Required	Sender_ID (sender)	Unique sender identifier
Required	SentDateTime (sent)	Date and time of the event For example: 2011-02-07T 16:49:00-05:00
Required	MessageStatus (status)	One of the following: <ul style="list-style-type: none"> <li>• Actual</li> <li>• Exercise</li> <li>• System</li> <li>• Test</li> <li>• Draft</li> </ul>
Required	MessageType (msgType)	One of the following: <ul style="list-style-type: none"> <li>• Alert</li> <li>• Update</li> <li>• Cancel</li> <li>• Ack</li> <li>• Error</li> </ul>
Optional	Source (source)	The source of the message
Required	Scope (scope)	Contains the value Public
Required	Code (code)	Contains the value KPI to hide this event from the Events portlet list.
Required	EventCategory (category)	One of the following: <ul style="list-style-type: none"> <li>• Geo</li> <li>• Met</li> <li>• Safety</li> <li>• Security</li> <li>• Rescue</li> <li>• Fire</li> <li>• Health</li> <li>• Env</li> <li>• Transport</li> <li>• Infra</li> <li>• CBRNE</li> <li>• Other</li> </ul>
Required	EventType (event)	Description of the event. For example: Police_Department_Budget
Required	Urgency (urgency)	One of the following: <ul style="list-style-type: none"> <li>• Immediate</li> <li>• Expected</li> <li>• Future</li> <li>• Past</li> <li>• Unknown</li> </ul>

Table 20. CAP elements used in IBM Intelligent Operations Center KPI calculations (continued)

Required or Optional	Data Element (normative)	Description
Required	Severity (severity)	One of the following: <ul style="list-style-type: none"> <li>• Extreme</li> <li>• Severe</li> <li>• Moderate</li> <li>• Minor</li> <li>• Unknown</li> </ul>
Required	Certainty (certainty)	One of the following: <ul style="list-style-type: none"> <li>• Observed</li> <li>• Likely</li> <li>• Possible</li> <li>• Unlikely</li> <li>• Unknown</li> </ul>
Optional	EventCode (eventCode)	Name value pairs for event typing.
Optional	OnsetDateType (onset)	Date time when the event started. For example: 2011-02-08T16:49:00-05:00
Optional	SenderName (senderName)	Name of the entity initiating the alert. For example: Police Department
Optional	EventDescription (description)	Detailed description of the event
Optional	Parameter (parameter)	Additional data associated with the event.
Optional	AreaGeocode (geocode)	A field that can be used to provide information when the KPI is location dependent

For more information, see the OASIS Common Alerting Protocol specification.

The following is an example of an event reporting a car accident.

```
<?xml version="1.0" encoding="UTF-8"?>
<cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:emergency:cap:1.2 CAP-v1.2-os.xsd ">
  <cap:identifier>1112</cap:identifier>
  <cap:sender>Transportation</cap:sender>
  <cap:sent>2011-02-17T15:00:00-05:00</cap:sent>
  <cap:status>Actual</cap:status>
  <cap:msgType>Alert</cap:msgType>
  <cap:scope>Public</cap:scope>
  <cap:code>KPI</cap:code>
  <cap:info>
    <cap:category>Transport</cap:category>
    <cap:event>Traffic_Accident</cap:event>
    <cap:urgency>Unknown</cap:urgency>
    <cap:severity>Extreme</cap:severity>
    <cap:certainty>Unknown</cap:certainty>
    <cap:eventCode>
      <cap:valueName>OwningOrg</cap:valueName>
      <cap:value>Police</cap:value>
    </cap:eventCode>
    <cap:onset>2011-02-17T15:00:00-05:00</cap:onset>
    <cap:senderName>Transportation</cap:senderName>
    <cap:description>Single car crash</cap:description>
    <cap:parameter>
```

```
<cap:valueName>accident number</cap:valueName>
<cap:value>1112</cap:value>
</cap:parameter>
</cap:info>
</cap:alert>
```

#### Related information:

 [OASIS Common Alerting Protocol Version 1.2](#)

## Using CAP for non-KPI events

CAP data can also be used to provide data on events not associated with KPI calculations.

CAP data received by the IBM Intelligent Operations Center that is not associated with defined KPIs will be added to the Events and Map portlets in the IBM Intelligent Operations Center.

## Configuring the IBM Intelligent Operations Center to receive events

External event queues messages are received by the IBM Intelligent Operations Center on an inbound queue. The messages must follow the Common Alerting protocol.

To configure event communication in the IBM Intelligent Operations Center, you must:

- Define the queue for event messages being sent to the IBM Intelligent Operations Center.
- Structure event messages sent to the queue according to CAP.

For more information, see the links at the bottom of the topic.

#### Related concepts:

“Using the inbound event queue defined for the IBM Intelligent Operations Center”

CAP events can be published into the IBM Intelligent Operations Center by directing them to the included WebSphere Message Broker instance.

“Integrating with the Common Alerting Protocol” on page 61

The Common Alerting Protocol (CAP) is used to exchange event information between the IBM Intelligent Operations Center and external systems.

## Using the inbound event queue defined for the IBM Intelligent Operations Center

CAP events can be published into the IBM Intelligent Operations Center by directing them to the included WebSphere Message Broker instance.

Publishing clients can be configured to point directly to the WebSphere Message Broker CAP event input queue, or they can use the WebSphere Application Server JMS resources defined on the portal server.

These JMS resources point to the WebSphere Message Broker queue that receives CAP events. The following JMS resources are created when the IBM Intelligent Operations Center is installed:

- Queue Connection Factory
  - Name: ioc.mb.con.factory
  - JNDI Name: jms/ioc.mb.con.factory
- Queue
  - Name: ioc.cap.in.q
  - JNDI Name: jms/ioc.cap.in.q

### Related concepts:

“Configuring the IBM Intelligent Operations Center to receive events” on page 68

External event queues messages are received by the IBM Intelligent Operations Center on an inbound queue. The messages must follow the Common Alerting protocol.

## Integrating with other protocols

Products and services that do not support the Common Alerting Protocol (CAP) can integrate with the IBM Intelligent Operations Center.

To integrate with IBM Intelligent Operations Center using other protocols, an adapter must be written to convert those protocols to the CAP.

### Related information:



OASIS Common Alerting Protocol Version 1.2

---

## Publishing CAP messages

The IBM Intelligent Operations Center provides the Sample Publisher portlet as an automated test tool and provides additional publishing capabilities as a service.

In addition to the IBM Intelligent Operations Center, there are two tiers of service provided with the IBM Intelligent Operations Center:

- Publisher servlet
- Publisher utility class

## Sample Publisher

Use the Sample Publisher portlet to publish Common Alerting Protocol (CAP) events into the IBM Intelligent Operations Center.

### What is the Sample Publisher portlet?

The Sample Publisher portlet is an automated test tool intended for an administrator managing or verifying the solution. It serves as a client application for testing the publication of CAP messages in the IBM Intelligent Operations Center. The Sample Publisher portlet can eliminate the requirement to manually create a test client application.

### What does the Sample Publisher portlet display?

On the **Sample Events** tab of the Sample Publisher portlet, you can complete a form to design events with XML. Submit the form to activate a flow of sample CAP events into the system.

The Sample Publisher portlet also contains a **New Event** tab for creating new events when it is not necessary to edit the XML. Complete the form in the **New Event** tab to submit the CAP event details. If you want to create new events with properties based on the properties of an existing event, enter the ID for the existing event in the **CAP Alert ID** field.

On the **Notifications** tab, you can complete a form to submit an alert notification for specified groups. The **Send To Group** field must match one of the existing user groups, for example, CitywideExecutives, because only matching alerts are displayed in the Coordinator - Alerts portlet list.

### Random values

On the **Sample Events** tab, if you select the **Randomize Events** check box, the portlet automatically alters the properties of the events it publishes as follows:

- **ID:** the portlet generates a unique ID string for each event because event IDs must be unique in the IBM Intelligent Operations Center.
- **Timestamp:** The portlet increments the value of the timestamp for each event sent so that each event in the sequence arrives at a different time.
- **Location:** The portlet randomizes the latitude and longitude for each event, within a range, to comply with the format required for latitude, longitude, and radius; for example, 32.9525,-115.5527 5. The radius setting is not changed.

**Related tasks:**

“Verifying the solution installation” on page 33

You can verify that the IBM Intelligent Operations Center is correctly installed and configured.

## Creating sample events with XML

On the **Sample Events** tab, you can select a sample CAP event template that you can use to view, modify, and publish events.

### About this task

Initially, choose an event category. The categories represent the primary areas into which events are divided.

*Table 21. Event categories*

Category	Description
CBRNE	Chemical, biological, radiological, nuclear, or high-yield explosive threat or attack
Environmental	Pollution and other environmental event
Fire	Fire suppression and rescue
Geophysical	Geophysical event, including landslide
Health	Medical and public health event
Infrastructure	Utility, telecommunication, or other non-transport infrastructure event
Meteorological	Meteorological event, including flood
Rescue	Rescue and recovery
Safety	General emergency and public safety
Security	Law enforcement, military, homeland, and local/private security
Transportation	Public and private transportation
Other	Other events

### Procedure

1. Click the **Sample Events** tab.
2. In the **Category** list, select an event category.
3. In the **Sample Event** list, select an event . In the **Event Message** field, the XML for the corresponding prewritten CAP message is inserted automatically.
4. Optional: Optionally, in the **Event Message** field, edit the XML for the prewritten CAP message.
5. In the **Event Instance Count** field, select the number of messages required. You can submit a single CAP message or an automated sequence of messages.
6. Optional: Optionally, select the **Randomize Events** check box. If you select **Randomize Events**, when a sequence of CAP messages is published certain properties are automatically assigned random values.
7. Click **Submit Event**.

## Results

The Sample Publisher populates the IBM Intelligent Operations Center with events and can trigger KPIs.

### Creating new CAP events without XML

On the **New Event** tab, you can complete a form to create new CAP events without using XML.

#### About this task

You can use the form to create either a new event or an event based on the values from an existing event. When you create an event based on an existing event, you use the CAP Identifier value to reference the existing event. If you do not know the CAP Identifier value for an existing event, you can use the Incident value instead. Any values that you enter on the form override values from the existing CAP event.

#### Procedure

1. Click the **New Event** tab.
2. To specify a source for the event, next to Source click one of the following options:
  - To create a new event with values based on the values you enter in the form, click **New**.
  - To create an event with values based on an existing event in the CAP events table and using the CAP Identifier, click **Existing**.
  - To create an event with values based on an existing event in the CAP events table and using the Incident value, click **Incident**.
3. In the **ID** field, enter an ID depending on whether you are creating a new event, or an event based on an existing CAP Identifier or Incident value:
  - If you are creating a new event, optionally enter a value for **ID**. If you do not enter a value, a unique identifier is generated for you.
  - If you are creating an event based on an existing CAP Identifier value, enter the CAP Identifier value for **ID**. Any values that you enter on the form override values from the existing CAP event.
  - If you are creating an event based on an existing Incident value, enter the Incident value for **ID**. Any values that you enter on the form override values from the existing CAP event.
4. In the **Headline** field, enter a headline.
5. From the **Category** list, select a category.
6. From the **Urgency** list, select the urgency.
7. From the **Severity** list, select the severity.
8. From the **Certainty** list, select the certainty.
9. In the **Description** field, enter a description.
10. In the **Sender** field, enter a description of the sender of the event.
11. In the **Event Instance Count** field, select the number of messages required. You can submit a single CAP message or an automated sequence of messages.
12. Optional: Optionally, select the **Randomize Events** check box. If you select **Randomize Events**, when a sequence of CAP messages is published certain properties are automatically assigned random values.
13. Click **Submit Event**.

#### Testing notifications

You can use the **New Notification** tab to create IBM Intelligent Operations Center notifications.

## About this task

On the **New Notification** tab, complete the form to submit an alert for specified groups. Ensure that one of the values that you enter in the **Sent To Groups** field matches one of the groups that you are a member of, for example, City-wide Executives or City-wide Operators. The reason for this is that only matching alerts are displayed in the City Coordinator - Alerts portlet list. When you create an alert on the **New Notification** tab, the new alert is written directly into the NOTIFICATION table in the IBM Intelligent Operations Center database and the City Coordinator - Alerts portlet list is notified to refresh.

## Procedure

1. Click the **New Notification** tab.
2. To create an alert, from the **Type** list, select **Alert**.
3. Optional: Optionally, from the **Category** list, select a category.
4. Optional: Optionally, in the **Headline** field, enter a headline.
5. Optional: Optionally, in the **Description** field, enter a description.
6. Optional: Optionally, in the **Sender** field, enter a description of the sender of the event.
7. Optional: Optionally, in the **Sent to Groups** field, enter a semicolon separated list of groups to send the alert to.
8. Optional: Optionally, do one of the following steps as required:
  - In the **Refers to Alerts** field, enter a semicolon separated list of CAP event identifiers that the new alert refers to.
  - In the **Refers to KPIs** field, enter a semicolon separated list of KPIs that the new alert refers to.
9. Click **Submit Notification**.

---

## Customizing KPIs

Key performance indicators (KPIs) can be created and modified using the IBM WebSphere Business Monitor and the IBM WebSphere Business Monitor Development Toolkit.

This information center describes how to create and modify KPIs for use with the IBM Intelligent Operations Center using the IBM WebSphere Business Monitor Development Toolkit. The IBM WebSphere Business Monitor Development Toolkit can be installed with Rational Application Developer, which is also shipped with IBM Intelligent Operations Center. The IBM WebSphere Business Monitor Development Toolkit can also be installed with WebSphere Integration Developer.

Before defining or modifying a KPI you must understand the Common Alerting Protocol (CAP) alert the KPI will be based on. For example, if you are defining a KPI tracking the level of a water source, you will need to know the CAP elements containing the elements that need to be tracked, such as the name of the water source and the water depth in feet.

After a KPI is added or modified it must be deployed to the IBM WebSphere Business Monitor server.

For additional information on using the IBM WebSphere Business Monitor and the IBM WebSphere Business Monitor Development Toolkit, see the IBM WebSphere Business Monitor information center.



**Related concepts:**

“Sample KPIs” on page 83

Sample KPIs are provided with the IBM Intelligent Operations Center. The KPIs are designed to provide guidance for implementing different types of KPIs using the IBM WebSphere Business Monitor Development Toolkit. Samples monitor models are provided for water, transportation and public safety.

“Creating KPIs for use with the IBM Intelligent Operations Center” on page 93

Key Performance Indicators (KPIs) are handled by events within the IBM Intelligent Operations Center. They are used to drive statistical data that can be used to analyze trends or to indicate problem areas.

**Related tasks:**

“Deploying monitor models” on page 81

After defining key performance indicators (KPIs) and their monitor models, the monitor models need to be deployed to the IBM WebSphere Business Monitor running on the IBM Intelligent Operations Center analytic server.

**Related reference:**

“Installing tools provided with the solution” on page 23

Toolkits and development tools are included with the IBM Intelligent Operations Center. These are used when customizing the IBM Intelligent Operations Center.

**Related information:**

 [IBM Business Monitor information center](#)

## Monitor models and KPIs

A monitor model defines metrics and key performance indicators (KPIs), their dependencies on incoming events, conditions requiring business actions, and the outbound events reporting the conditions that might trigger business actions.

A monitor model can contain the following sub-models:

- Monitor details model
- KPI model
- Dimensional model
- Visual model
- Event model

The monitor details model contains most of the monitor model information.

The sample monitor models provided by the IBM Intelligent Operations Center do not use the visual or dimensional models.

The monitor details model defines one or more monitoring contexts. A monitoring context defines the information to be collected and monitored from one or more incoming events. For the IBM Intelligent Operations Center monitored entities are CAP alerts. The information collected from these alerts is used to calculate a KPI.

The KPI model contains one or more KPI contexts. These define the KPIs and their associated triggers and events. KPI contexts can process inbound events, evaluate recurring wait-time triggers and send outbound events. For example, the context can check if a KPI is out of the defined range and send a notification.

The event model refers to all event inbound and outbound definitions used in the monitor model. It refers to schemas describing the structure of individual event parts.

**Related concepts:**

“Sample KPIs” on page 83

Sample KPIs are provided with the IBM Intelligent Operations Center. The KPIs are designed to provide guidance for implementing different types of KPIs using the IBM WebSphere Business Monitor Development Toolkit. Samples monitor models are provided for water, transportation and public safety.

**Related information:**

 [IBM Business Monitor information center](#)

## Monitoring context instances

A monitoring context instance is information collected at a specific point in time within a monitoring context.

For the IBM Intelligent Operations Center a monitoring context instance is analogous to a CAP alert. When a CAP alert is received, a monitoring context instance is created or reused and the metrics within that context instance are populated with the CAP alert values based on the monitoring context.

A monitoring context can be defined to create a new instance for each CAP alert or to reuse an existing instance. For example, if you want a KPI to calculate the average weekly water level for a given resource with the water level sampled daily, you would create a new monitor context instance for each CAP alert. Each instance would contain the daily water level and the KPI would average the measurements over the seven day period.

KPIs are calculated using the metrics defined for a monitoring context. When defining an aggregation KPI, you specify the monitoring context and metric used as input to the KPI aggregation function. When the KPI is evaluated, the metric values for the monitoring context instances are used by the aggregation function to calculate the KPI value.

**Related concepts:**

“Sample KPIs” on page 83

Sample KPIs are provided with the IBM Intelligent Operations Center. The KPIs are designed to provide guidance for implementing different types of KPIs using the IBM WebSphere Business Monitor Development Toolkit. Samples monitor models are provided for water, transportation and public safety.

**Related information:**

 [IBM Business Monitor information center](#)

## Modeling KPIs

Model KPIs using Rational Application Developer or WebSphere Integration Developer with the IBM WebSphere Business Monitor Developers toolkit installed. Rational Application Developer and the IBM WebSphere Business Monitor Developers toolkit are included as part of the IBM Intelligent Operations Center.

**About this task**

KPIs are modeled using Rational Application Developer or WebSphere Integration Developer with the IBM WebSphere Business Monitor Developers toolkit. For more information on using these tools, see the information centers for these products.

Monitoring models are contained within business monitoring projects. Models and projects are created using the Rational Application Developer business monitor wizards provided by the IBM WebSphere Business Monitor Developers toolkit.

To model a KPI, do the following.

## Procedure

1. Understand the CAP alert to be received by the IBM Intelligent Operations Center.
2. Understand the purpose of the KPI. Will the KPI generate an action if a limit is reached or exceeded? Will the KPI be used to calculate historical or statistical data?
3. Determine the name for the monitoring context. The IBM Intelligent Operations Center naming convention is to use the CAP event type as the name. The samples provided by IBM Intelligent Operations Center create separate monitoring context for each CAP alert message sent to the IBM WebSphere Business Monitor.
4. In the Rational Application Developer with the IBM WebSphere Business Monitor Developers toolkit installed, define the inbound event, key and set of metrics for the monitor context. The inbound event defines the CAP alert message monitored by the context, a key uniquely defining the context instance, and the metrics defining the information extracted from the CAP alert message.
5. Specify the CAP schema for the event. The schema must exist in the monitoring project. The IBM Intelligent Operations Center provides a copy of the CAP v1.2 schema in the sample `icoc_sample_monitor_models` modeling project.
6. Specify the name and ID for each business monitor inbound event. Event IDs cannot contain spaces or special characters. By default the ID is created from the name with underscores substituted for spaces. All samples provided by the IBM Intelligent Operations Center use default element IDs.
7. Specify the schema. The schema defines the structure of the inbound event to the IBM WebSphere Business Monitor.
8. Define any desired filtering of CAP messages. For example, limit monitoring to specific event types or severity.
9. Specify the metrics to be extracted from the CAP message.
10. Define a context key to uniquely identify the monitoring context instance. Key values are specified by the inbound event when the monitoring context is created.
11. Specify whether inbound events should be correlated.
12. Specify the KPI context. A KPI context is a container for KPIs and their associated triggers and events. Unlike a monitoring context, a KPI context contains no keys or metrics. A KPI context must be created as a container before creating any KPIs.
13. Create the KPI within the previously defined KPI context.
14. Specify the type of KPI: **Decimal** or **Duration**.
15. Define the KPI ranges, values, and color indicators. Most of the sample IBM Intelligent Operations Center KPIs define three ranges and associated colors.

Table 22. Sample KPI range and color definitions

Name	Color	RGB
acceptable	green	e4f2d1
caution	yellow	fee881
take action	red	e68b88

16. Define how the KPI value is calculated. KPI values are determined in one of two ways. If the value comes from a metric using an aggregation function, the KPI is referred to as an aggregation KPI. If the value is calculated based on other KPIs or user-defined XPath functions, the KPI is referred to as an expression KPI.

In the IBM Intelligent Operations Center samples the lowest level KPIs (those without children) are defined as aggregation KPIs. The higher level KPIs (KPIs with children) are defined as expression KPIs.

Aggregation KPI values are calculated from metrics populated with data sent in CAP alert messages sent to the IBM WebSphere Business Monitor server. An aggregation function is then run on this data. Aggregation functions include:

- average
- maximum
- minimum
- sum
- number of occurrences
- standard deviation

The values are expressed as quantifiable measurements. For example, average crime response time (5 minutes, 7 seconds) or average water level (100.5).

Expression KPI values are calculated from KPI ranges and calculations. In the IBM Intelligent Operations Center samples the parent KPIs have calculations causing the KPI to evaluate to a value of 0, 1, or 2 depending on the values of their child KPIs. A value of 0 maps to the acceptable range, 1 to the caution range, and 2 to the take action range. The samples use calculation expressions to set the KPI value to the highest urgency of its children.

17. Optional: Specify the time filter for an aggregation KPI. Aggregation KPIs can have optional time filters limiting the period of time over which the KPI value is calculated. The time period can be a repeating interval (for example, the last completed or current period), a rolling interval, or a fixed interval. All sample IBM Intelligent Operations Center aggregation KPIs have defined time filters.
18. Optional: Specify a data filter for the KPI. For example, if the average crime response time is to be calculated for Police Precinct One and no other precinct, a data filter can be used to remove all other monitoring contexts.
19. Define how the KPI values are updated including triggers, events inbound to the IBM WebSphere Business Monitor server and outbound events to the IBM Intelligent Operations Center.
20. Test the KPI.
21. Deploy the monitor model application.

**Related concepts:**

“Nested KPIs”

While IBM WebSphere Business Monitor allows a KPI based on the value of another KPI, it does not allow the definition of a parent/child relationship between KPIs. Defining parent/child relationships must be done in the IBM Intelligent Operations Center.

“Sample KPIs” on page 83

Sample KPIs are provided with the IBM Intelligent Operations Center. The KPIs are designed to provide guidance for implementing different types of KPIs using the IBM WebSphere Business Monitor Development Toolkit. Samples monitor models are provided for water, transportation and public safety.

“KPI event communication between the IBM WebSphere Business Monitor and the IBM Intelligent Operations Center” on page 78

The IBM WebSphere Business Monitor can send outbound events from a monitoring or key performance indicator (KPI) context to the IBM Intelligent Operations Center.

**Related tasks:**

“Deploying monitor models” on page 81




After defining key performance indicators (KPIs) and their monitor models, the monitor models need to be deployed to the IBM WebSphere Business Monitor running on the IBM Intelligent Operations Center analytic server.

**Related reference:**

“Installing tools provided with the solution” on page 23

Toolkits and development tools are included with the IBM Intelligent Operations Center. These are used when customizing the IBM Intelligent Operations Center.

**Related information:**

-  IBM Business Monitor information center
-  Rational Application Developer information center
-  XML Path Language (XPath) 2.0 (Second Edition)

## Nested KPIs

While IBM WebSphere Business Monitor allows a KPI based on the value of another KPI, it does not allow the definition of a parent/child relationship between KPIs. Defining parent/child relationships must be done in the IBM Intelligent Operations Center.

The IBM Intelligent Operations Center sample KPIs define a series of Police Department KPIs.

```

Police Department ----- level 1
  Crime Response Time ----- level 2
    Crime Response Time Precinct One ----- level 3
    Crime Response Time Precinct Two ----- level 3

```

In this case Police Department has one child: Crime Response Time. Crime Response Time has two children: Crime Response Time Precinct One and Crime Response Time Precinct Two.

The two level 3 KPIs are defined as aggregation KPIs. That is, their values are calculated using a metric value and an aggregation function. All other KPIs in this set are expression KPIs with their values calculated from the values of the other KPIs. For example:

- Crime Response Time is based on the values of Crime Response Time Precinct One and Crime Response Time Precinct Two.
- Police Department is based on the value of Crime Response Time.

### Related concepts:

“Defining KPI parent/child relationships”

KPI parent/child relationships are defined in a Web Ontology Language (OWL) document which is read and processed by the IBM Intelligent Operations Center.

## Defining KPI parent/child relationships

KPI parent/child relationships are defined in a Web Ontology Language (OWL) document which is read and processed by the IBM Intelligent Operations Center.

For example, the OWL definitions for the Police Department KPI set are:

```
<icop:KPIDefinition rdf:ID="Police_Department">
<icop:KPIBase.name>Police Department</icop:KPIBase.name>
<icop:KPIBase.id>Police_Department</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_ModelDefinition
  rdf:resource= "#icoc_sample_public_safety_monitor_model"/>
</icop:KPIDefinition >
```

```
<icop:KPIDefinition rdf:ID="Crime_Response_Time">
<icop:KPIBase.name>Crime Response Time</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Police_Department"/>
</icop:KPIDefinition >
```

```
<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_One">
<icop:KPIBase.name>Crime Response Time Precinct One</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_One</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >
```

```
<icop:KPIDefinition rdf:ID="Crime_Response_Time_Precinct_Two">
<icop:KPIBase.name>Crime Response Time Precinct Two</icop:KPIBase.name>
<icop:KPIBase.id>Crime_Response_Time_Precinct_Two</icop:KPIBase.id>
<icop:KPIDefinition.isChildOf_KPIDefinition rdf:resource= "#Crime_Response_Time"/>
</icop:KPIDefinition >
```

### Related concepts:

“Nested KPIs” on page 77

While IBM WebSphere Business Monitor allows a KPI based on the value of another KPI, it does not allow the definition of a parent/child relationship between KPIs. Defining parent/child relationships must be done in the IBM Intelligent Operations Center.

## KPI event communication between the IBM WebSphere Business Monitor and the IBM Intelligent Operations Center

The IBM WebSphere Business Monitor can send outbound events from a monitoring or key performance indicator (KPI) context to the IBM Intelligent Operations Center.

Outbound events from the IBM WebSphere Business Monitor server are placed on an external message queue. The IBM Intelligent Operations Center uses this mechanism to asynchronously receive KPI updates.

### Related concepts:

“Using the inbound event queue defined for the IBM Intelligent Operations Center” on page 68  
CAP events can be published into the IBM Intelligent Operations Center by directing them to the included WebSphere Message Broker instance.

## Triggers

A trigger is a mechanism that detects an occurrence and can cause additional processing in response to that occurrence.

The KPI samples provided with the IBM Intelligent Operations Center define two types of triggers. The first trigger is fired when a CAP alert message, also known as an inbound event, is received by the IBM WebSphere Business Monitor server for a defined KPI set. The CAP alert message might, or might not, change the KPI. The IBM Intelligent Operations Center determines if the KPI is changed when it receives the event notification from the IBM WebSphere Business Monitor server.

For outbound events, a trigger determines when the event will be sent.

Event based triggers can be used to send notifications to the IBM Intelligent Operations Center when input for a KPI calculation changes. However, event triggers cannot be used to address the situation when a KPI value changes after a defined time period expires. In the IBM Intelligent Operations Center samples, time based triggers are used to send notifications to the IBM Intelligent Operations Center for those KPIs with short time period definitions.

For example, the Severe Traffic Accidents KPI is defined to expire every hour. If the KPI has a value of 3 at 10:00 and no CAP alert messages are received for that KPI during the next hour, then the time period expires and the KPI value is reset to 0.

## **Defining inbound events to IBM WebSphere Business Monitor**

In the IBM Intelligent Operations Center samples, inbound events are used to determine when a trigger is fired. Inbound events for a KPI context are defined in a similar manner to those for a monitoring context.

### **About this task**

Inbound events are defined using Rational Application Developer or WebSphere Integration Developer with the IBM WebSphere Business Monitor Developers toolkit. For more information on using these tools, see the information centers for these products.

To define an inbound event, do the following.

### **Procedure**

1. Select the KPI context for the inbound event.
2. Create the inbound event and specify the event name and ID.
3. Specify the CAP schema.
4. Specify the filter condition.
5. Select the KPI context and create a new inbound event.
6. Create a new trigger for the inbound event.
7. Make sure that the trigger is repeatable so the trigger fires each time the trigger source is updated and the trigger condition is met.
8. Select the trigger source.
9. Define the trigger condition. When the trigger condition is met, the trigger fires.

### **Example**

The sample IBM Intelligent Operations Center monitor models are defined so that a trigger fires each time a CAP alert message is received by the IBM WebSphere Business Monitor server.

## Related tasks:

“Modeling KPIs” on page 74

Model KPIs using Rational Application Developer or WebSphere Integration Developer with the IBM WebSphere Business Monitor Developers toolkit installed. Rational Application Developer and the IBM WebSphere Business Monitor Developers toolkit are included as part of the IBM Intelligent Operations Center.

## Related information:

 [IBM Business Monitor information center](#)

 [Rational Application Developer information center](#)

## Defining outbound events to the IBM Intelligent Operations Center

Outbound events define the information sent from the IBM WebSphere Business Monitor to the IBM Intelligent Operations Center when a trigger fires.

### About this task

The IBM Intelligent Operations Center uses outbound notifications sent from the IBM WebSphere Business Monitor server to determine if the KPI has changed. If the KPI has changed, the IBM Intelligent Operations Center obtains the KPI data from the IBM WebSphere Business Monitor server, updates the KPI cache information, and updates the IBM Intelligent Operations Center data.

Outbound events are defined using Rational Application Developer or WebSphere Integration Developer with the IBM WebSphere Business Monitor Developers toolkit. For more information on using these tools, see the information centers for these products.

To define an outbound event, do the following steps.

### Procedure

1. Select the KPI context for the outbound event.
2. Create the outbound event and specify the event name and ID.
3. Specify the notification schema. The schema is located in the `ioc-notification-v1.0.xsd` file. The schema is located in the `icoc_sample_monitor-models` project.
4. Define the content of the outbound event. The content is based on the notification schema.
5. Under **notification**, for the value of **sentfrom** enter Monitor.
6. Add the parameter elements to the event content, as defined in the following substeps:
  - a. For the first parameter, specify 'modelID' for **parameterName** and the monitor model ID for **parameterValue**. For example, `icoc_sample_public_safety_monitor_model`.
  - b. For each KPI in the KPI set, add parameters to specify the KPI ID and KPI value. The KPI ID is specified using the **parameterName** element and the KPI value is specified using the **parameterValue** element. The KPI ID must be associated with a KPI in the KPI set. Use the `xs:string()` function to specify the KPI value as a string. For example, **parameterName** can be `'Police_Department'` and **parameterValue** can be `xs:string(Police_Department)`.

### Example

The following is an example of a notification to be sent to the IBM Intelligent Operations Center:

```
<ns1:notification>
  <ns1:notificationType> Alert</ns1:notificationType>
  <ns1:sentFrom> Monitor</ns1:sentFrom>
  <ns1:headline> Police Department KPI Changed</ns1:headline>
  <ns1:description> Police Department KPI Changed</ns1:description>
  <ns1:kpiLink> Police Department</ns1:kpiLink>
  <ns1:category> Safety</ns1:category>
```



```

<ns1:parameter>
  <ns1:parameterName> modelId</ns1:parameterName>
<ns1:parameterValue>
  icoc_sample_public_safety_monitor_model</ns1:parameterValue>
</ns1:parameter>
<ns1:parameter>
  <ns1:parameterName> Police_Department</ns1:parameterName>
  <ns1:parameterValue> 0</ns1:parameterValue>
</ns1:parameter>
<ns1:parameter>
  <ns1:parameterName> Crime_Response_Time</ns1:parameterName>
  <ns1:parameterValue> 0</ns1:parameterValue>
</ns1:parameter>
<ns1:parameter>
  <ns1:parameterName> Crime_Response_Time_Precinct_One</ns1:parameterName>
  <ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
</ns1:parameter>
<ns1:parameter>
  <ns1:parameterName> Crime_Response_Time_Precinct_Two</ns1:parameterName>
  <ns1:parameterValue> PT3M30.000S</ns1:parameterValue>
</ns1:parameter>
</ns1:notification>

```

### Related tasks:

“Modeling KPIs” on page 74

Model KPIs using Rational Application Developer or WebSphere Integration Developer with the IBM WebSphere Business Monitor Developers toolkit installed. Rational Application Developer and the IBM WebSphere Business Monitor Developers toolkit are included as part of the IBM Intelligent Operations Center.

### Related information:



IBM Business Monitor information center



Rational Application Developer information center

## Deploying monitor models

After defining key performance indicators (KPIs) and their monitor models, the monitor models need to be deployed to the IBM WebSphere Business Monitor running on the IBM Intelligent Operations Center analytic server.

### About this task

To deploy a monitor model that will be used by the IBM WebSphere Business Monitor, Java Enterprise Edition (JEE) projects must be generated from the defined models. Once the JEE projects are generated, the model application can be exported as an EAR file. The EAR file can then be deployed into the IBM WebSphere Business Monitor running on the IBM Intelligent Operations Center analytic server.

### Procedure

1. In Rational Application Developer or WebSphere Integration Developer with the IBM WebSphere Business Monitor Developers toolkit installed, right-click the monitor model requiring project generation in the **Enterprise Explorer** tab. For example, `icoc_sample_public_safety_monitor_model`.
2. Click **Generate Monitor JEE Projects**. The following projects will be created: `modelApplication`, `modelLogic`, and `modelModerator`.
3. Export the monitor model application by right-clicking the `modelApplication` project and clicking **Export > EAR**.
4. Test the KPIs before deploying the EAR file into IBM WebSphere Business Monitor.
5. Deploy the EAR file into the IBM WebSphere Business Monitor server using the instructions in the IBM WebSphere Business Monitor information center.

## Related information:

 [IBM Business Monitor information center](#)

 [Rational Application Developer information center](#)

## KPI display values

The IBM Intelligent Operations Center resource bundles can be used to provide alternate display values from those values provided by the IBM WebSphere Business Monitor models.

KPI display names and range names are defined in the sample IBM WebSphere Business Monitor models provided with the IBM Intelligent Operations Center. Examples of KPI display names are:

- Water
- Water Quality

Examples of range names are:

- acceptable status value
- caution status value
- take action status value

Each artifact, for example KPI and range, defined in IBM WebSphere Business Monitor has an ID associated with the display name. IDs cannot contain spaces while display values can. The IDs are used as keys to look up values in a resource bundle. The IBM Intelligent Operations Center uses these IDs to select KPI display values. If no values are specified in the resource bundle for the ID, the value specified in the IBM WebSphere Business Monitor definition are used.

The KPI display values are localized by IBM WebSphere Business Monitor using the ISO language and country codes of the IBM WebSphere Business Monitor server. For example, a KPI percentage value would be displayed in the format 12.61% for when the locale is en\_US and 12,61% when the locale is fr\_FR. Resource bundle definitions are not used for these values.

The default IBM Intelligent Operations Center properties resource bundle is `com.ibm.iss.icoc.rest.monitor.resources.Messages.properties`. The bundle can be found in `icoc_rest_monitor_resources_utils`.

This is an example resource bundle:

```
kpi.NO.VALUE=No data to determine the KPI value
kpi.RANGE.UNDETERMINED=undetermined
Flood_Control=Flood Control
Water_Levels=Water Levels
Flow_Discharge_City_River=Flow Discharge City River
Water_Level_City_Lake=Water Level City Lake
```

In this example, the values of `kpi.NO.VALUE` and `kpi.RANGE.UNDETERMINED` are used by the IBM Intelligent Operations Center when the IBM WebSphere Business Monitor KPIs return a null value. For example, the Water Level City Lake KPI is defined with a repeating daily time period based on the last full period. If no CAP events are received for that KPI on a Sunday, and the KPI is requested on Monday, null is returned since no data is available for the previous day. The display value is set to "No data to determine the KPI value" and the range display name is set to "undetermined".

The other entries, `Flood_Control`, `Water_Levels`, `Flow_Discharge_City_River`, and `Water_Level_City_Lake`, define the display values for the KPI IDs defined in the `icoc` sample water monitor model provided by the IBM Intelligent Operations Center. These entries can specify alternate text from the values specified in the IBM WebSphere Business Monitor monitor. For example, the resource bundle can be used to provide translated values instead of changing the model itself.

**Related concepts:**

“Sample KPIs”

Sample KPIs are provided with the IBM Intelligent Operations Center. The KPIs are designed to provide guidance for implementing different types of KPIs using the IBM WebSphere Business Monitor Development Toolkit. Samples monitor models are provided for water, transportation and public safety.

## Caching KPIs

IBM Intelligent Operations Center configuration settings affect when KPI settings are retrieved from the IBM WebSphere Business Monitor.

By default, the IBM Intelligent Operations Center loads KPIs into a cache and refresh the cache every two hours.

For most KPIs this refresh time is sufficient to deliver updated KPIs to the IBM Intelligent Operations Center. If there are KPIs defined with time periods shorter than two hours, or there are KPIs that are frequently updated, the default cache refresh interval might be insufficient.

**Related concepts:**

“Specifying system-wide configuration data” on page 91

The IBM Intelligent Operations Center SYSPROP table stores IBM Intelligent Operations Center configuration data.

---

## Sample KPIs

Sample KPIs are provided with the IBM Intelligent Operations Center. The KPIs are designed to provide guidance for implementing different types of KPIs using the IBM WebSphere Business Monitor Development Toolkit. Samples monitor models are provided for water, transportation and public safety.

The lowest level KPIs are defined as aggregation KPIs. Aggregation KPIs are calculated from values contained in incoming CAP alert messages and an aggregation function such as average, maximum, minimum, sum, number of occurrences, or standard deviation. Their values are expressed as quantifiable measurements. Hover text is used to display actual KPI values. Lower level KPI values are localized into the appropriate format based on the locale of the IBM WebSphere Business Monitor server. The higher level KPIs are mapped to values based on how the mapping is defined in the sample KPI.

The value of the higher level sample KPI is a number which equates to color and the level of response recommended (0 is acceptable, 1 is monitoring, and 2 is action). The value of the lowest level KPI is a duration, a decimal, a percentage or a currency depending on the KPI it represents. For example:

- 15% is the actual value of a KPI representing the percentage of delayed flights at a particular airport over a period of time.
- 5 minutes, 7 seconds is the actual value of a KPI representing the average crime response time for a given location over a period of time.

The source files for the sample IBM Intelligent Operations Center monitor models are provided in an archive file that can be imported into Rational Application Developer or WebSphere Integration Developer with the IBM WebSphere Business Monitor Toolkit installed. The archive file can be modified to change, add, or delete KPI definitions. The definitions can then be regenerated and redeployed to the IBM Intelligent Operations Center.

The sample models shipped with the IBM Intelligent Operations Center are:

- `icoc sample public safety monitor model`
- `icoc sample transportation monitor model`
- `icoc sample water monitor model`

These models contain the following KPI samples:

- Water
  - Flood Control
    - Water Levels
      - Flow Discharge City River
      - Water Level City Lake
  - Water Management
    - Strategical Planning
      - Water Leakage
      - Water Supply vs Demand
  - Water Quality
    - Physical Indicators
      - Turbidity
      - pH
- Transportation
  - Airports
    - Delayed Flights
      - Delayed Flights Airport One
      - Delayed Flights Airport Two
  - Roads and Traffic
    - Road Events
      - Severe Traffic Accidents
  - Transportation Management
    - Revenue
      - Bridges and Tunnel Tolls
      - Parking Facilities Revenue
- Public Safety
  - Fire Department
    - Firefighter Injuries
      - Firefighter Injuries Fire Station One
      - Firefighter Injuries Fire Station two
  - Police Department
    - Crime Response Time
      - Crime Response Time Precinct One
      - Crime Response Time Precinct Two
  - Public Safety Management
    - Public Safety Budget
      - EMS Department Budget
      - Fire Department Budget
      - Police Department Budget

**Related concepts:**

“Status” on page 109

Use the Status portlet to see the status of key performance indicators (KPIs) for a single organization or across organizations.

“Key Performance Indicator Drill Down” on page 110

Use the Key Performance Indicator Drill Down portlet to see additional information about a KPI, the status and values of its underlying KPIs, and its calculation time.

“Customizing KPIs” on page 72

Key performance indicators (KPIs) can be created and modified using the IBM WebSphere Business Monitor and the IBM WebSphere Business Monitor Development Toolkit.

**Related tasks:**

“Deploying monitor models” on page 81

After defining key performance indicators (KPIs) and their monitor models, the monitor models need to be deployed to the IBM WebSphere Business Monitor running on the IBM Intelligent Operations Center analytic server.

---

## Creating reports

The IBM Intelligent Operations Center provides a reporting subsystem using IBM Cognos Business Intelligence to create and manage reports.

The reporting subsystem is installed on the analytic server by the IBM Intelligent Operations Center deployment wizard. An IBM Cognos Business Intelligence model is provided with the IBM Intelligent Operations Center interim fix PO00001. You can use this supplied model to create your own reports.

For more information on creating reports using the supplied model, see the IBM Cognos Business Intelligence information center.

**Related concepts:**

“System configuration” on page 9

The IBM Intelligent Operations Center installs and configures an environment with production servers and one server used during the installation process.

**Related information:**

 [IBM Intelligent Operations Center interim fix PO00001](#)

 [IBM Cognos Business Intelligence information center](#)



---

## Chapter 5. Customizing the solution

Customizing the solution to suit your particular operation includes the tasks covered in this section in relation to the user interface and system properties table. Customizing is closely related to integrating the solution and the appropriate links are included in event and key performance indicator (KPI) topics in this section.

---

### Customizing the user interface

You can customize elements of the IBM Intelligent Operations Center user interface to suit your operation

As well as customizing the layout and appearance of portlets, you can also create new pages. For more information, see the WebSphere Portal product documentation.

#### Related information:



[IBM WebSphere Portal Product Documentation](#)

### Localizing the user interface

Browser settings determine language, date and time settings for the IBM Intelligent Operations Center user interface. An administrator can customize the date and time formats.

In the IBM Intelligent Operations Center, your browser settings determine the language of the text. Where that language is unavailable in the IBM Intelligent Operations Center, the closest relation is used; for example, French Canadian reverts to French which in turn reverts to English which is always available. Your browser settings also determine the time zone for all dates and times that are displayed. Date and time in IBM Intelligent Operations Center are automatically adjusted to the browser's time zone.

All dates and times are presented in your time zone in the format specified in the SYSPROP database table. System properties hold the date and time format strings. To change the value in the database by editing the property, follow the link at the end of the topic.

#### Related concepts:

[“Specifying system-wide configuration data” on page 91](#)

The IBM Intelligent Operations Center SYSPROP table stores IBM Intelligent Operations Center configuration data.

### List of portlets

IBM Intelligent Operations Center is a portlet-based solution that uses portal technology to provide tools and display information. All the portlets included in IBM Intelligent Operations Center are listed.

The portlets included in the IBM Intelligent Operations Center are described in the following table. The table also indicates in which views each portlet is available.

*Table 23. Portlets in the IBM Intelligent Operations Center*

Portlet	Description	User views
<a href="#">“Status” on page 109</a>	The Status portlet provides an executive-level summary of the status of KPIs across the organizations that you have permission to view. Use this portlet to view up-to-date changes in the KPI status so that you can plan and take action if necessary.	Executive

Table 23. Portlets in the IBM Intelligent Operations Center (continued)

Portlet	Description	User views
“Key Performance Indicator Drill Down” on page 110	When you see a KPI category in the Status portlet that needs attention, select it. All of the KPIs for the category you selected are then displayed in the Key Performance Indicator Drill Down portlet. You can use this list to inspect the underlying KPIs until you reach details of the KPI that caused the status change.	Executive
“Coordinator - Alerts” on page 111	The Coordinator - Alerts portlet provides a dynamic, interactive list of alerts that result from changing KPIs and correlated events. The role of this portlet is to draw attention to changes in KPI or event status. The list contains key details for each of the alerts.	Executive, Operations
“Sametime Contacts” on page 113	The Sametime Contacts portlet provides a contacts list organized by group. It can be customized based on the people you need to communicate with. You can chat with people and modify your online status, contacts, or groups.	Executive, Operations
“Map” on page 114	In the Map portlet:  A map of the geographical region provides event location information.  An input form selects which categories of event are shown on the map and in the Events portlet list.	Operations
“Events” on page 117	The Events portlet provides a list of events. The list contains key details for each of the events. You can display a more detailed description of an event by hovering over the row in the list.	Operations
Sample Publisher	The Sample Publisher portlet is an automated test tool intended for an administrator managing or verifying the solution. It serves as a client application for testing the publication of CAP messages in the IBM Intelligent Operations Center. The Sample Publisher portlet can eliminate the requirement to manually create a test client application.	Administration
Security	The Security portlet is provided as an administrative and test tool that displays details of group membership and permissions that have been granted to users.	Administration



Table 23. Portlets in the IBM Intelligent Operations Center (continued)

Portlet	Description	User views
Intelligent Operations Center - About	The About portlet displays details of the version of IBM Intelligent Operations Center you have installed.	Administration

## Customizing the page layout

You can customize the appearance and layout of the portlets included in the IBM Intelligent Operations Center.

### About this task

Use the WebSphere Portal user interface to customize portlets:

#### Procedure

1. To open WebSphere Portal, click the **Administration** tab.
2. In WebSphere Portal, click **Portal User Interface**.
3. In the Portal User Interface, click the required option:
  - To register themes and skins, set the default theme, and set the default skin for each theme, click **Themes and Skins**.
  - To customize the key site elements in themes, including the banner, navigation, fonts, and colors, click **Theme Customizer**.
4. Make the required modifications. For more information about using WebSphere Portal to customize portlets, see the link at the bottom of the topic for the WebSphere Portal product documentation.

#### Related information:

 [IBM WebSphere Portal Product Documentation](#)

## Configuring the map

An administrator can configure the map view for all users. You can set the center point and zoom level for the map. The center point can be adjusted to specific longitude and latitude coordinates. You can also select the base map that the user sees. Select your installed Esri GIS server or a publicly available GIS service, for example, ArcGIS.com.

### About this task

To implement your map setting changes follow the procedure. Sample settings showing how the map can be configured are provided in the link at the end of the topic.

Hover over an icon to view hover help indicating the purpose of the icon.

#### Procedure

1. Log on to `http://portalServer/wps/myportal` as an administrative user.
2. On the navigation bar at the top of the page, click **Administration**.
3. On the sidebar menu, click **Portlet Management > Portlets**.
4. Locate the Map portlet and click **Configure portlet** (wrench icon).
5. Modify the configuration as required.
6. Click **OK** to save the modified configuration.

**Related concepts:**

“Map” on page 114

Use the Map portlet to see where events are located on a map and to control which categories of events are shown.

**Sample map configuration**

Sample settings for base map, map center point and map zoom level provide an example of how the map can be configured. Valid settings are supplied where applicable.

This table provides an example of how you can configure the map settings. It also specifies valid settings. Detailed steps for the task of configuring the map are explained in the link at the end of the topic.

*Table 24. Accepted values and examples of map configuration settings*

Setting	Accepted values	Preference setting	Example value
The center point for the map with values for latitude and longitude respectively	Valid latitude and longitude coordinates	com.ibm.iss.map.centerLat	-11.3
		com.ibm.iss.map.centerLon	-50
The zoom level for the map with a zoom level value	Valid range of zoom levels is determined by the base map. Generally, the range is from 1 upwards. The value of 1 is the lowest zoom level which displays the map at its lowest magnification. The default base map supplied with IBM Intelligent Operations Center, ArcGIS, displays geographical detail up to a maximum of zoom level 12.	com.ibm.iss.map.zoom	4
The base map with values for the map type and the map URL respectively	The valid map type is ARC_GIS_REST.	com.ibm.iss.map.baseMap.type	ARC_GIS_REST
		com.ibm.iss.map.baseMap.Url	http://services.arcgisonline.com/ArcGIS/rest/services/World_Street_Map/MapServer/tile/{z}/{y}/{x}

## Specifying system-wide configuration data

The IBM Intelligent Operations Center SYSPROP table stores IBM Intelligent Operations Center configuration data.

The following are system-wide properties used by the IBM Intelligent Operations Center.

Table 25. System-wide SYSPROP values used by the IBM Intelligent Operations Center

Realm	Subject	Name	Type	Value
System	*	DateFormat	String	The format used when the IBM Intelligent Operations Center displays the date. The default is yyyy-MM-dd. Any valid Java <code>java.text.SimpleDateFormat</code> date pattern can be specified.
System	*	DateTimeFormat	String	The format used when the IBM Intelligent Operations Center displays the date and time. The default is yyyy-MM-dd HH:mm:ss. Any valid Java <code>java.text.SimpleDateFormat</code> date and time pattern can be specified.
System	*	ModelManagerServerEJBPort	String	The EJB port used by model manager.
System	*	ModelManagerServerHostname	String	The host name or IP address used by model manager.
System	*	MonitorServerHostname	String	The host name or IP address used by IBM WebSphere Business Monitor.
System	*	MonitorServerWebPort	String	The web port used by IBM WebSphere Business Monitor REST Services Gateway.
System	*	PortalServerHostname	String	The host name or IP address used by WebSphere Portal Server.
System	*	PortalServerWebPort	String	The web port used by WebSphere Portal Server.
System	*	RegExpEmail	System	The regular expression used to validate an e-mail address. The default is <code>\b[a-zA-Z0-9._%~]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,6}\b</code> .
System	*	RegExpTelephone	System	The regular expression used to validate a telephone number. The default is <code>[\w]+</code> .
System	*	SecurityUserPrefix	String	The user ID prefix used to map the user to the LDAP distinguished name. The default is <code>uid</code> .
System	*	SecurityUserSuffix	String	The user ID suffix used when mapping the user to a local distinguished name.
System	*	TimeFormat	String	The format used when the IBM Intelligent Operations Center displays the time. The default is HH:mm:ss. Any valid Java <code>java.text.SimpleDateFormat</code> time pattern can be specified.
System	*	TSRMServerHostname	String	The Tivoli Service Request Manager host name.
System	*	TSRMServerWebPort	String	The web port used by Tivoli Service Request Manager.

Table 25. System-wide SYSPROP values used by the IBM Intelligent Operations Center (continued)

Realm	Subject	Name	Type	Value
System	*	TSRMServerWorkflowUri	String	The workflow URI used by Tivoli Service Request Manager. The default is /maximo/ui/?event=loadapp&value=sr&&additionalevent=useqbe&additionaleventvalue=TICKETID={0}. The CAP incident value is substituted for {0}.

The following can be changed to configure how KPIs are processed.

Table 26. SYSPROP values affecting KPI processing

Realm	Subject	Name	Type	Value
KPI	*	CacheKpis	Boolean	Specifies whether or not KPIs retrieved from IBM WebSphere Business Monitor are cached.  If false, KPIs are always retrieved from IBM WebSphere Business Monitor when the IBM Intelligent Operations Center requests KPI information.  If true, KPIs are cached for reuse. How often the cache is refreshed is specified by KpiCacheRefreshInterval.  The default is true.
KPI	*	KpiCacheRefreshInterval	Integer	Specifies how often the KPI cache is refreshed. The interval is specified in minutes. KpiCacheRefreshInterval is ignored if CacheKpis is specified as false.
KPI	*	KpiSentToGroup	String	Specifies the groups that receive KPI notifications. Separate group names with a semicolon (;). The default is CityWideExecutive;CityWideSupervisor.
KPI	*	PreLoadKpis	Boolean	Specifies if the KPIs are retrieved from IBM WebSphere Business Monitor when the IBM Intelligent Operations Center starts.  If false, KPIs are retrieved from IBM WebSphere Business Monitor only when the IBM Intelligent Operations Center requests KPI information.  If true, all KPIs are retrieved from IBM WebSphere Business Monitor when the IBM Intelligent Operations Center is started. The KPIs are cached for reuse. How often the cache is refreshed is specified by KpiCacheRefreshInterval. <b>Note:</b> If PreLoadKpis is true, CacheKpis is assumed to be true regardless of its specified value.  The default is true.

You can change the following SYSPROP values to configure event correlation. Event correlation values determine if the IBM Intelligent Operations Center identifies if multiple events will affect one another due to their time or proximity.

Table 27. SYSPROP values affecting event correlation

Realm	Subject	Name	Type	Value
Impact	Correlation	Distance	Float	The distance between events that might impact one another. The default is 5. The distance unit is specified by UnitOfDistance.

Table 27. SYSPROP values affecting event correlation (continued)

Realm	Subject	Name	Type	Value
Impact	Correlation	TimeWindow	Float	The amount of time between events that might impact one another. The value is in hours. The default is 2.
Impact	Correlation	UnitOfDistance	String	The unit of distance used with the Distance value. Valid values are mile and kilometer.

**Important:** If any of the Impact SYSPROP values are changed, the Tivoli Netcool/Impact server on the event and management server must be restarted to make those changes effective.

**Related concepts:**

“Policy for event correlation” on page 61

The event correlation policy determines if the IBM Intelligent Operations Center identifies events affecting one another due to their time or proximity.

## Updating the SYSPROP table

To change system-wide IBM Intelligent Operations Center configuration data, update the SYSPROP table.

### About this task

**Important:** The following procedure reloads the IBM Intelligent Operations Center database and deletes all existing IBM Intelligent Operations Center data. Deleted data includes all existing Common Alerting Protocol (CAP) events and alerts. To update a system-wide property without losing existing data in the solution, manually update the SYSPROP table.

### Procedure

1. On the database server, edit the following file:  
`/op/IBM/iss/ioc/db/IOC_PopulateSysPropTables.sql`
2. Make the required changes.
3. Save the file.
4. Run the following command:  
`/opt/IBM/iss/ioc/db/createIOCDB_db2.sh`

---

## Creating KPIs for use with the IBM Intelligent Operations Center

Key Performance Indicators (KPIs) are handled by events within the IBM Intelligent Operations Center. They are used to drive statistical data that can be used to analyze trends or to indicate problem areas.

The IBM Intelligent Operations Center provides a set of sample KPIs and events that can be used to update KPI status. Each IBM Intelligent Operations Center installation must define the KPIs required for their environment. For more information, see the link at the end of the topic.

**Related concepts:**

“Customizing KPIs” on page 72

Key performance indicators (KPIs) can be created and modified using the IBM WebSphere Business Monitor and the IBM WebSphere Business Monitor Development Toolkit.

---

## Configuring IBM Cognos Business Intelligence to create reports in IBM Intelligent Operations Center

IBM Intelligent Operations Center provides a reporting subsystem that uses IBM Cognos Business Intelligence to create and manage reports. Before you use IBM Cognos Business Intelligence to create and manage reports, you must configure IBM Intelligent Operations Center.

The reporting subsystem is installed on the analytic server and uses an analytic data model.

### Setting up an IBM Cognos Business Intelligence data source

To set up an IBM Cognos Business Intelligence data source, you must catalog the database, and then create the data source in IBM Cognos Connection.

**Related concepts:**

“Importing the IBM Intelligent Operations Center analytics data model into IBM Cognos Business Intelligence” on page 95

To import the IBM Intelligent Operations Center analytics data model into IBM Cognos Business Intelligence, you must copy the IBM Intelligent Operations Center analytics data model to the IBM Cognos Business Intelligence server, and then copy the analytics data model into IBM Cognos Connection.

### Cataloging the database

**About this task**

To catalog the database, use the following procedure:

**Procedure**

1. To log in to the IBM Cognos Business Intelligence server as a DB2 user, in a command window, enter the following command: `su - db2inst1`
2. To catalog the DB2 node that contains the IBM Intelligent Operations Center event database, enter the following command:

```
db2 catalog tcpip node iocdb remote fully-qualified server name server 50000
```

A message is displayed telling you that the command completed successfully.

3. To catalog the actual database on the DB2 node, enter the following command:

```
db2 catalog database iocdb as iocdb at node iocdb
```

A message is displayed telling you that the command completed successfully.

**What to do next**

Create a data source in IBM Cognos Connection.

### Creating a data source in IBM Cognos Connection

**About this task**

To create a data source, use the following procedure:

## Procedure

1. Open IBM Cognos Connection at <http://analytic server name/9082/p2pd/servlet /dispatch/ext>.
2. To log in, for **User ID** enter `wpsadmin` and enter the password, then click **OK**.
3. In the top navigation bar, click **Launch**.
4. In the drop-down list, select **IBM Cognos Administration**.
5. Click the **Configuration** tab.
6. To create a new data source, near the top right corner, click the database icon. The first screen of the New Data Source wizard is displayed.
7. For **Name**, enter `IOC`, and then click **Next**. The data model supplied with the IBM Intelligent Operations Center requires the data source name.
8. For **Type**, select **IBM DB2**, and then click **Next**.
9. For **DB2 database name**, enter `IOCDB`.
10. For **DB2 connect string**, enter `jdbc:db2://DB2_server:50000/IOCDB`, where `DB2_server` is the name of your DB2 server.
11. To enable passwords, in the Signons section, select the **Password** checkbox.
12. For **User ID**, **Password** and **Confirm password**, enter values for the IOCDB database.
13. In the Testing section, click **Test the connection**.
14. To run the connection test, click **Test**. If the connection test is successful, a message is displayed indicating that the **Status** is Succeeded.
15. To close the test results page, click **Close**.
16. To close the test page, click **Close**.
17. Near the bottom of the **Configuration** tab, click **Next**.
18. To finish and save your data source, click **Finish**.

## What to do next

Import the IBM Intelligent Operations Center analytics data model into IBM Cognos Business Intelligence.

## Importing the IBM Intelligent Operations Center analytics data model into IBM Cognos Business Intelligence

To import the IBM Intelligent Operations Center analytics data model into IBM Cognos Business Intelligence, you must copy the IBM Intelligent Operations Center analytics data model to the IBM Cognos Business Intelligence server, and then copy the analytics data model into IBM Cognos Connection.

### Related concepts:

“Setting up an IBM Cognos Business Intelligence data source” on page 94

To set up an IBM Cognos Business Intelligence data source, you must catalog the database, and then create the data source in IBM Cognos Connection.

## Copying the IBM Intelligent Operations Center analytics data model to the IBM Cognos Business Intelligence server Before you begin

Set up an IBM Cognos Business Intelligence data source.

## Procedure

To copy the analytics data model to the IBM Cognos Business Intelligence server, copy the `ioc_analytics_data_model.zip` file to the `/opt/ibm/cognos/c10_64/deployment` directory.

## What to do next

Copy the IBM Intelligent Operations Center analytics data model into IBM Cognos Connection.

## Importing the IBM Intelligent Operations Center analytics data model into IBM Cognos Connection

### About this task

To copy the analytics data model into IBM Cognos Connection, use the following procedure.

### Procedure

1. Open IBM Cognos Connection at `http://analytic server name:9082/p2pd/servlet /dispatch/ext`.
2. To log in, for **User ID** enter `wpsadmin` and the password, then click **OK**.
3. In the top navigation bar, click **Launch**.
4. In the drop-down list, select **IBM Cognos Administration**.
5. Click the **Configuration** tab.
6. In the left menu, click **Content Administration**.
7. To import a new data model, near the top right corner, click the import a new data model icon. The first screen of the New Import wizard is displayed.
8. In the Deployment archive screen, verify that the analytics data model that you copied to the IBM Cognos Business Intelligence server is selected, and then click **Next**.
9. Click **Next**.
10. In the Public folders screen, verify that the analytics data model that you copied to the IBM Cognos Business Intelligence server is selected, and then click **Next**.
11. In the options screen, click **Next**.
12. In the summary screen, click **Next**.
13. Because it is only necessary to import the analytics data model once, in the actions screen, click **Save and run once**, and then click **Finish**.
14. In the run screen, click **Run**.
15. Click **OK**. The analytics data model is imported.
16. In the top navigation bar, click **Launch**.
17. In the drop-down list, select **IBM Cognos Connections**. The analytics data model is listed in the **Public Folders** tab.
18. To see a list of available reports, in the list, click the analytics data model.
19. To run a report, click a report. The report is displayed.



---

## Chapter 6. Managing the solution

The topics in this section describe how to perform administrative tasks for IBM Intelligent Operations Center.

---

### Intelligent Operations Center - About

Use the Intelligent Operations Center - About portlet to view details of the version of the IBM Intelligent Operations Center and the integrated IBM Smarter Cities Software Solutions that you have installed.

The About portlet is provided as an upgrading or troubleshooting tool to display the version of the IBM Intelligent Operations Center you have installed and any updates you have applied since installation.

This portlet can be found on the **Administration** view by clicking **Verification Tools > Intelligent Operations Center - About**.

#### Related tasks:

“Verifying the solution installation” on page 33

You can verify that the IBM Intelligent Operations Center is correctly installed and configured.

---

### Controlling components with IOControl

You can control or query the status of the IBM Intelligent Operations Center components by using the **IOControl** command.

The **IOControl** command can be run from the event and management server. The **IOControl** script file is located in `/opt/IBM/ISP/mgmt/scripts`.

**Fix Pack 1** When you successfully install the IBM Intelligent Operations Center 1.0 Fix Pack 1, a new **IOControl** script file is located in `/opt/IBM/ISP/mgmt/scripts`. The old **IOControl** script file is located in `/opt/IBM/ISP/mgmt/backup`.

Components of the IBM Intelligent Operations Center have interdependencies requiring that they start and stop in a specific order. The required order is implemented by the **IOControl** command. If you need to restart any physical machine, VM, or component; it is good practice to stop and then start all of the IBM Intelligent Operations Center components. It is possible to use the **IOControl** command to stop and start components individually, but this use of the command is not recommended.

### Getting help for the IOControl command

Information about action and target options for the **IOControl** command is available.

#### Procedure

On the event and management server run one of the following commands to see options for the **IOControl** command.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh help
```

or

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh
```

## Results

The options for the **IOControl** command are displayed. The list is similar to the list that is shown in the example.

Fix Pack 1

### Example

The **IOControl** command help for the IBM Intelligent Operations Center 1.0 Fix Pack 1 is as follows:

```
[root@OpCentert1s6 scripts]# /opt/IBM/ISP/mgmt/scripts/IOControl.sh help
Usage: IOControl.sh action target password
Action options:
  start          -      Start server
  stop           -      Stop server
  status         -      Check server status
  help          -      Get help message
Target options:
  all            -      All Middleware servers
  db24po        -      IBM DB2 Enterprise server for Portal Server
  db24app       -      IBM DB2 Enterprise server for Application Server
  db24rt        -      IBM DB2 Enterprise server for Runtime
  db24ana       -      IBM DB2 Enterprise server for Analytics Server
  db24mg        -      IBM DB2 Enterprise server for Management Server
  *db24tsrm    -      IBM DB2 Enterprise server for TSRM Server
  tds           -      IBM Tivoli Directory Server
  tamps         -      IBM Tivoli Access Manager Policy Server
  tamas         -      IBM Tivoli Access Manager Authorization Server
  tamwpm        -      IBM Tivoli Access Manager Web Portal Manager
  tamweb        -      IBM Tivoli Access Manager WebSEAL
  teps          -      IBM Tivoli Monitoring Enterprise Monitoring Server
  tepts         -      IBM Tivoli Monitoring Enterprise Portal Server
  isk           -      IBM Solutions Kit Core Server
  tim           -      IBM Tivoli Identity Manager
  was           -      IBM WebSphere Application Server for Runtime
  *cplex        -      IBM WebSphere Application Server for CPLEX
  ihs           -      IBM HTTP Server for Runtime
  ncob          -      IBM Tivoli Netcool OMNIBus
  nci           -      IBM Tivoli Netcool Impact
  wbm           -      IBM WebSphere Business Monitor
  st            -      IBM Lotus Sametime
  wpe           -      IBM WebSphere Portal Extend
  wmb           -      IBM WebSphere Message Broker
  mih           -      IBM Master Information Hub
  cognos        -      IBM COGNOS Business Intelligence
  *tsrm         -      IBM Tivoli Service Request Manager [root@OpCentert1s6 scripts]#
```

**Note:** Fix Pack 1

For the IBM Intelligent Operations Center 1.0 Fix Pack 1, there are three new targets for the IOControl script, denoted by an asterisk in the preceding list.

## Starting components

A script is available to start the IBM Intelligent Operations Center components.

### Procedure

On the event and management server, run the following command to start all the IBM Intelligent Operations Center components.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh start all password
```

where *password* is the password for the IBM Intelligent Operations Center administrator defined when the IBM Intelligent Operations Center was deployed.

## Results

The IBM Intelligent Operations Center components are started.

## What to do next

After the IBM Intelligent Operations Center components are started, start the Tivoli Netcool/OMNIBus probe.

## Starting the Tivoli Netcool/OMNIBus probe

Start the Tivoli Netcool/OMNIBus probe after all IBM Intelligent Operations Center servers have been started.

## About this task

On the event and management server, run the following commands.

### Procedure

1. Run

```
mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log
```

2. Run

```
/opt/IBM/netcool/omnibus/probes/nco_p_xml -name ioc_xml -propsfile /opt/IBM/netcool/omnibus/probes/linux2x86/ioc_xml.props &
```

## Stopping components

A script is available to stop the IBM Intelligent Operations Center components.

### Procedure

On the event and management server, run the following command to start all the IBM Intelligent Operations Center components.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh stop all password
```

where *password* is the password for the IBM Intelligent Operations Center administrator defined when the IBM Intelligent Operations Center was deployed.

## Results

The IBM Intelligent Operations Center components are stopped.

## Querying the status of components

A script is available to determine the status of IBM Intelligent Operations Center components.

### Procedure

On the event and management server run the following command to query the status of all the IBM Intelligent Operations Center components.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status all password
```

where *password* is the password for the IBM Intelligent Operations Center administrator defined when the IBM Intelligent Operations Center was deployed.

To check only one component, run the following command.

```
/opt/IBM/ISP/mgmt/scripts/IOControl.sh status component_ID password
```

where *server\_ID* is an ID listed under **Target Options** in the **IOControl** help and *password* is the password for the IBM Intelligent Operations Center administrator defined when the IBM Intelligent Operations Center was deployed.

## Results

Components that are started are shown with the indicator **on**. Components that are not started are shown with the indicator **off**.

---

## Fix pack server monitoring

Fix Pack 1

View the data collected by the Tivoli Enterprise Monitoring Agent.

### About this task

Tivoli Enterprise Monitoring Agents are installed and running on each of the IBM Intelligent Operations Center servers. In the Tivoli Enterprise Portal client, you can view data monitored and collected by the Tivoli Enterprise Monitoring Agents.

### Procedure

1. Open the Tivoli Enterprise Portal browser client at `http://event and management server:1920///cnp/client`.
2. In the **Warning - Security** dialog, click **Yes**.
3. To log on, enter your user ID and password. The default user ID is `sysadmin`, with no password required.
4. On the left of the window, the **Navigator** view shows the monitored servers with a list of the types of agents installed. These agents also have various subagents. You can click the agents or subagents to display the related workspace. The workspace is composed of many views showing the status collected by the agent as a table or a diagram. For example, under the **management server** node in the **Navigator** view, the **Linux OS Agent** has **Disk Usage**, **Process**, and other subagents. Select **Process** to open a new workspace with a set of views for process.

#### Related concepts:

“What’s new in the fix pack?” on page 6

The IBM Intelligent Operations Center 1.0 Fix Pack 1 delivers stability improvements, upgrades to components, and system-monitoring infrastructure.

#### Related reference:

 Tivoli Enterprise Portal User's Guide

## Starting and stopping server monitoring

Fix Pack 1

You can start or stop each Tivoli Enterprise Monitoring Agent if required because of performance or other concerns.

### About this task

Tivoli Enterprise Monitoring Agents are installed on each IBM Intelligent Operations Center server. Using the commands in the table, you can start or stop Tivoli Monitoring.

The agents on each server are listed in Table 28.

The commands to start or stop each Tivoli Enterprise Monitoring Agent are listed in Table 29

Table 28. Monitoring agents on each server

Server	Agents for
Access server	Red Hat Enterprise Linux
Portal server	Red Hat Enterprise Linux, DB2 Enterprise Server Edition, WebSphere Application Server, IBM HTTP Server, Lotus Domino, Lotus Sametime Entry
Application and integration server	Red Hat Enterprise Linux, DB2 Enterprise Server Edition, WebSphere Application Server, WebSphere Message Broker, WebSphere MQ
Database server	Red Hat Enterprise Linux, DB2 Enterprise Server Edition,
Analytic server	Red Hat Enterprise Linux, DB2 Enterprise Server Edition, WebSphere Application Server
Event and management server	Red Hat Enterprise Linux, DB2 Enterprise Server Edition, WebSphere Application Server
Tivoli Service Request Manager server	Red Hat Enterprise Linux, DB2 Enterprise Server Edition, WebSphere Application Server, IBM HTTP Server

Table 29. Tivoli Enterprise Monitoring Agent commands

Agent for	Command
Red Hat Enterprise Linux	/opt/IBM/ITM4LNX/bin/itmcmd agent start lz /opt/IBM/ITM4LNX/bin/itmcmd agent stop lz
WebSphere Application Server	/opt/IBM/ITM4WAS/bin/itmcmd agent start yn /opt/IBM/ITM4WAS/bin/itmcmd agent stop yn
DB2 Enterprise Server Edition	/opt/IBM/ITM/bin/itmcmd agent -o db2inst1 start ud /opt/IBM/ITM/bin/itmcmd agent -o db2inst1 stop ud
IBM HTTP Server	/opt/IBM/ITM/bin/itmcmd agent start ht /opt/IBM/ITM/bin/itmcmd agent stop ht
Lotus Domino,	/opt/IBM/ITM/bin/itmcmd agent -o domino_agent_1 start gb /opt/IBM/ITM/bin/itmcmd agent -o domino_agent_1 stop gb
Lotus Sametime Entry	/opt/IBM/ITM/bin/itmcmd agent -o sametime1 start s1 /opt/IBM/ITM/bin/itmcmd agent -o sametime1 stop s1
WebSphere Message Broker,	/opt/IBM/ITM/bin/itmcmd agent start qi /opt/IBM/ITM/bin/itmcmd agent stop qi
WebSphere MQ	/opt/IBM/ITM/bin/itmcmd agent start mc /opt/IBM/ITM/bin/itmcmd agent -o IOC.MB.QM start mq /opt/IBM/ITM/bin/itmcmd agent stop mc /opt/IBM/ITM/bin/itmcmd agent -o IOC.MB.QM stop mq

## Managing the heartbeat service

### Fix Pack 1

The heartbeat service provided with the IBM Intelligent Operations Center 1.0 Fix Pack 1 restarts middleware components if they fail.

## About this task

The heartbeat service on the event and management server checks the status of middleware components. If a middleware component fails, the failure triggers the heartbeat service to restart the middleware component. You can enable or disable this function using the commands provided.

**Note:** The heartbeat service is enabled by default after the fix pack is installed. For details of components the service operates on, see the related concept link at the end of the topic.

## Procedure

1. Log on to the event and management server as root.
2. Disable the heartbeat service using the following command:  

```
/opt/IBM/ISP/heartbeat/scripts/control_heartbeat.sh disable
```

## What to do next

To enable the heartbeat service, log on as in the procedure and use the following command:

```
/opt/IBM/ISP/heartbeat/scripts/control_heartbeat.sh enable
```

### Related concepts:

“What’s new in the fix pack?” on page 6

The IBM Intelligent Operations Center 1.0 Fix Pack 1 delivers stability improvements, upgrades to components, and system-monitoring infrastructure.

---

## Maintaining the solution

Perform the tasks described in this section to keep your solution running smoothly.

## Tuning performance

The following sections describe how to tune the portal server and WebSphere Application Server.

### Tuning the portal server

#### About this task

Use the following guidelines, which are based on the results of performance tests, to set the Java Virtual Machine heap size.

#### Procedure

1. Set the minimum and maximum heap sizes to the same values.
2. Set the heap size to a value that is compatible with the physical memory and that is above 2 GB.

#### What to do next

For more information, see the Portal Server 7 Performance Tuning Guide.

### Tuning WebSphere Application Server

For information on tuning the performance of WebSphere Application Server Version 7, see the WebSphere Application Server, Network Deployment, Version 7.0 Information Center.

## Managing log files

IBM Intelligent Operations Center stores log files in several different locations. To prevent system performance issues, periodically archive log files and remove the original log files.

If you do not manage log files and the number of log files increases indefinitely, the log files can eventually fill up a file system partition. Filling up a file system partition might have negative consequences and potentially cause the system to stop.

See the link at the end of the topic for information about the log files that are available in IBM Intelligent Operations Center.

**Related concepts:**

“Log files” on page 125

To troubleshoot a problem in IBM Intelligent Operations Center, you might need to analyze log files in several systems. The following topics list the log files that are available in IBM Intelligent Operations Center, and categorize the log files by server and system.

## Backing up data

To prevent the loss of valuable data in IBM Intelligent Operations Center, back up certain files, directories, and databases.

When you extend IBM Intelligent Operations Center, it is good practice to develop a backup procedure for the items you have added, for example:

- Reports
- Ancillary databases
- Database tables
- Custom analytics
- Portlets
- Java applications

Also consider data that you have accumulated, for example:

- Common Access Protocol (CAP) database data
- IBM WebSphere Business Monitor database data
- Lightweight Directory Access Protocol (LDAP) user registry data
- Geographical Information System (GIS) data

Adopt a naming convention to make it easier to identify the extensions you have added. In general, track the data that you have created or accumulated since you installed the original solution. Implement procedures for backing up the data, so that when you upgrade the solution, you do not lose valuable data.

The following table lists the files, directories, and databases that it is recommended you back up in IBM Intelligent Operations Center. The files, directories, and databases are grouped by the server where they are located.

*Table 30. IBM Intelligent Operations Center recommended backup files, directories, and databases*

Server	Files and directories			Database	
	Middleware	Path	Approximate Size	Instance name	Database name
Access server	WebSEAL	/opt/pdweb/etc	352 KB	No database	No database
		/opt/pdweb/ www-default/jct	16 KB		

Table 30. IBM Intelligent Operations Center recommended backup files, directories, and databases (continued)

Server	Files and directories			Database	
	Middleware	Path	Approximate Size	Instance name	Database name
Portal server	Portal server	/opt/IBM/ WebSphere/ wp_profile	1.1 GB	db2inst1	WPSDBJCR WPSDBCTM
	Sametime and Domino server	/local/notesdata	1.2 GB		WPSDBLKM WPSDBCMT WPSDBRLS WPSDBFBK
Application and integration server	IBM Integrated Information Core for model manager	/opt/IBM/ WebSphere/ AppServer/ profiles/ MIHCustom01	176 MB	db2inst1	MIHDB
		/opt/IBM/ WebSphere/ AppServer/ profiles/ MIHDmgr01	89 MB		
	WebSphere MQ	/var/mqm	259 MB		
	WebSphere Message Broker	/var/mqsi	2.8 MB		
Database server	Not applicable	Not applicable		db2inst1	IOCDB
Analytic server	IBM WebSphere Business Monitor	/opt/IBM/ WebSphere/ AppServer/ profiles/qmwas	2.1 GB	db2inst1	CXLOGDB CXCONTDB MONITOR
	IBM Cognos Business Intelligence	/opt/IBM/ WebSphere/ AppServer/ profiles/ CognosAppSrv01	369 MB		EVENT
Event and management server	Tivoli Access Manager	/opt/ PolicyDirector/ etc	628 KB	dsrdbm01	DSRDBM01
	WebSphere Application Server Network Deployment for IBM Solution Kit Core	/opt/IBM/ WebSphere/ AppServer/ profiles/ ISPAAppSrv01	108 MB	db2inst1	ISPDB
	WebSphere Application Server for Management	/opt/IBM/ WAS/ V6.1/ profiles/ ISPAAppSrv01	252 MB		
Total size	Approximately 6 GB. The size does not vary much as the file sizes are stable.			Approximately 4 GB-100 GB. The size might grow rapidly as more data is accumulated.	



## **Maintenance tips**

Additional tips for maintaining the solution are documented in the form of individual technotes in the IBM Support Portal.

The following link launches a customized query of the live Support knowledge base: [View all maintenance tips for IBM Intelligent Operations Center.](#)



---

## Chapter 7. Using the solution interface

The IBM Intelligent Operations Center is a web-based solution using portal technology. It can be accessed with any of the supported web browsers.

For details of which browsers are supported, see the detailed system requirements document at the following URL: IBM Intelligent Operations Center system requirements

---

### Logging on

Log on to access the IBM Intelligent Operations Center user interface.

#### Before you begin

Contact your local administrator to obtain your user ID and password. Your administrator is responsible for ensuring that you have the security access level appropriate to your role in your organization. Your administrator will also supply you with the web address (URL) for the IBM Intelligent Operations Center.

#### About this task

Use the following procedure to start a new browser session and access the IBM Intelligent Operations Center. You can also access the solution from other IBM Smarter Cities Software Solutions installed in your environment. From the main navigation bar at the top of the portal, select the **Intelligent Operations Center**.

#### Procedure

1. Enter the web URL into the address field of the browser.
2. On the server home page, enter your user ID and password.
3. Click **Log In**.
4. Select **Intelligent Operations Center** from the navigation bar at the top of the portal.

#### Results

The IBM Intelligent Operations Center home page is displayed in the web browser. Only the pages, features, and data that you have permission to access are available. Contact your administrator if you need additional access.

#### Related tasks:

“Logging off”

Log off to exit the IBM Intelligent Operations Center user interface and end the server session. By default, the **Log Out** link is located in the upper right corner of the IBM Intelligent Operations Center.

---

### Logging off

Log off to exit the IBM Intelligent Operations Center user interface and end the server session. By default, the **Log Out** link is located in the upper right corner of the IBM Intelligent Operations Center.

## Related tasks:

“Logging on” on page 107

Log on to access the IBM Intelligent Operations Center user interface.

---

## Viewing or editing your user profile

You can view or change the information in your user profile for the IBM Intelligent Operations Center.

### About this task

Your profile contains information previously entered by you or your administrator. You can update your profile by editing the information in attribute fields. For example, you can change your existing password to a new one.

Table 31. IBM Intelligent Operations Center user profile attributes

Attribute	Description	User can edit?
User ID*	An ID is assigned to each new user by the administrator for identification purposes.	No
Password*	A password is assigned by the administrator for security. The password must be unique and 5 to 60 characters in length. Valid passwords must contain only the characters a-z, A-Z, period ".", dash "-", and underscore "_".	Yes
First name	A first name, or given name, can be entered by the administrator or the user.	Yes
Last name*	A last name, or family name, is entered by the administrator.	Yes
Mail	An email address can be entered by the administrator or the user.	Yes

**Note:** Attributes marked with an asterisk are required for the successful creation of a new user, those attributes not marked with an asterisk are optional.

### Procedure

1. On the right of the top navigation bar, select **Edit My Profile**. The attributes for your profile are displayed.
2. To change your password:
  - a. Enter your current password (password text is not displayed).
  - b. In the **New Password** field and **Confirm Password** fields, enter your new password.
3. Enter or edit information in any of the remaining fields.
4. To submit your changes, click **OK**.

### Results

Your user profile is updated with any changes.

---

## Executive view

Use the Executive view to obtain a consolidated view of key performance indicators (KPIs) and alerts associated with the KPIs. The Executive view enables users with cross-organization responsibility to monitor, manage, and respond to status changes in relation to the key areas of organizational performance and well-being.

The Executive view is an interactive web page. It contains the following portlets, which you can think of as independent sections of the page that cooperate with one another to provide comprehensive information and interaction at the executive level:

Table 32. Executive view portlets

Portlet	Description
"Status"	The Status portlet provides an executive-level summary of the status of KPIs across the organizations that you have permission to view. Use this portlet to view up-to-date changes in the KPI status so that you can plan and take action if necessary.
"Key Performance Indicator Drill Down" on page 110	When you see a KPI category in the Status portlet that needs attention, select it. All of the KPIs for the category you selected are then displayed in the Key Performance Indicator Drill Down portlet. You can use this list to inspect the underlying KPIs until you reach details of the KPI that caused the status change.
"Coordinator - Alerts" on page 111	The Coordinator - Alerts portlet provides a dynamic, interactive list of alerts that result from changing KPIs and correlated events. The role of this portlet is to draw attention to changes in KPI or event status. The list contains key details for each of the alerts. For example, when a KPI changes status from yellow to red, an alert is sent to the Coordinator - Alerts portlet.
"Sametime Contacts" on page 113	The Sametime Contacts portlet provides a contacts list organized by group. It can be customized based on the people you need to communicate with. You can chat with people and modify your online status, contacts, or groups.

For help using each portlet, click the upper right corner of the portlet, and select **Help** from the menu displayed.

To resize a portlet, click the upper right corner of the portlet, and select options from the menu that is displayed, as follows:

- To expand the portlet to fill the page, click **Maximize**.
- To hide the portlet contents, other than its title bar, click **Minimize**.
- To restore a minimized or maximized portlet to its default view, click **Restore**.

## Status

Use the Status portlet to see the status of key performance indicators (KPIs) for a single organization or across organizations.

### What is the Status portlet?

The Status portlet provides an executive-level summary of the status of KPIs across the organizations that you have permission to view. Use this portlet to view up-to-date changes in the KPI status so that you can plan and take action if necessary.

### What does this portlet display?

Each row contains KPI information about an organization that is named in the first column of the table. Each organization and the KPI categories associated with it are represented by colored cells. The background color for a KPI reflects its status.

The background color code supplied with the IBM Intelligent Operations Center sample KPIs is set up as follows:

- Green indicates that everything is okay, based on the acceptable parameters for that KPI
- Yellow indicates caution or monitoring is required.
- Red indicates that action is recommended.
- Gray indicates that there is insufficient data available to calculate the KPI status.

The undetermined status indicates that there is no KPI value available for the defined time period. This situation occurs when the IBM Intelligent Operations Center has not received any messages for a given KPI in the specified time period. For example, the water level for a water source is calculated daily. If no water level message for that water source is received on a particular day, then there is no data to determine the KPI value.

When an underlying KPI changes, the change is reflected in the Status portlet. For example, one of the sample KPIs that determine the status of the Water Quality KPI changes status from acceptable to caution. The change is reflected in the portlet by a change in the background color of the Water Quality cell from green to yellow. In addition, the Coordinator - Alerts portlet indicates that a KPI has changed.

When the solution receives a message related to the calculation of a KPI, there is an instant color change. This is an advantage when the KPI is one that is likely to receive changes in real time, such as airport delays or traffic accidents. It is not relevant to historical KPIs, such as flood control, where regular daily measurements are taken and there is unlikely to be sudden change effecting status in the interim.

To display all the underlying KPIs and their details in the Key Performance Indicator Drill Down portlet, click a colored table cell in the Status portlet.

For more information about using the solution interface, click **Help** in the upper right corner of the browser page.

For more information about administering and customizing the solution, go to the IBM Intelligent Operations Center Information Center .

## Key Performance Indicator Drill Down

Use the Key Performance Indicator Drill Down portlet to see additional information about a KPI, the status and values of its underlying KPIs, and its calculation time.

### What is the Key Performance Indicator Drill Down portlet?

When you see a KPI category in the Status portlet that needs attention, select it. All of the KPIs for the category you selected are then displayed in the Key Performance Indicator Drill Down portlet. You can use this list to inspect the underlying KPIs until you reach details of the KPI that caused the status change.

### What does this portlet display?

The Key Performance Indicator Drill Down portlet shows all the underlying KPIs associated with the organization or KPI category you have selected in the Status portlet. The KPIs are displayed in the form of a nested list that can be expanded or collapsed. The status of each underlying KPI is represented by color, in the same way that color is used for the KPIs displayed in the Status portlet. The underlying KPIs control the color of the parent KPI. To display the actual value of the KPI, hover over the KPI with your cursor. For example, the actual value for Severe Traffic Accidents is 10, an underlying for the Transportation Management KPI.

### Working with the list of KPIs

You can perform the tasks in the following list from the action bar at the top of the portlet. To view the action associated with an icon, place your mouse over the icon.

- To refresh the contents of the list, click **Refresh**.
- To select all the KPIs on the list, click **Select All**.
- To deselect all the KPIs on the list, click **Deselect All**.
- To collapse an expanded list, click **Collapse All**.
- To sort the list alphabetically, click the name of the column to be sorted.
- To revert a sorted list to unsorted, click **Clear Sort**.
- To select which columns to display, click **Configure Options** and select check boxes.
- To select which rows to display, enter text in the **Quick Filter** field to filter rows according to the text you define. The button to the left of the field allows you to clear the filter.

For more information about using the solution interface, click **Help** in the upper right corner of the browser page.

## Sample KPIs

### Administrator

A set of sample KPIs is provided with IBM Intelligent Operations Center. These KPIs are designed to provide guidance for planning and implementing different types of KPIs to suit your organization. Examples are provided in the areas of water, transportation, and public safety.

For more information about this subject, go to the IBM Intelligent Operations Center Information Center and search for sample KPIs. Also, see the information center for further information about administering and customizing the solution.

## Coordinator - Alerts

Use the Coordinator - Alerts portlet to view your alert messages and their details.

### What is the Coordinator - Alerts portlet?

The Coordinator - Alerts portlet is an interactive window containing a list of all the current alerts relevant to you. You see only alerts that have been sent to your user groups. Alerts are notifications received when:

- Multiple events are happening in the same vicinity and at a similar time, thus might be in conflict or require coordination
- A predefined key performance indicator (KPI) value change occurs, where that change has been defined as an alert trigger by your administrator

You can also use the Coordinator - Alerts portlet to display further details of an alert.

### What does this portlet display?

The Coordinator - Alerts portlet provides a dynamic, interactive list of alerts that result from changing KPIs and correlated events. The role of this portlet is to draw attention to changes in KPI or event status. The list contains key details for each of the alerts.

To show a more detailed description of an alert, hover over the row with the cursor. To see all the information associated with that alert in a pop-up window, right-click the row and select **Properties**.

Initially, when you open the portal page, the Coordinator - Alerts portlet displays all of your current alerts. Remove any alert from the portlet by right-clicking the row and selecting **Close alert**. It is possible to close multiple alerts in this way by selecting multiple rows. Close an alert only after you have handled it appropriately because the alert is removed for all recipients when you close it.

Click the button in the upper right corner of the pop-up window to cancel it and take you back to the list.

## Alert Properties

The pop-up window for alert details displays the following properties:

Table 33. Alert properties

Property	Content
Headline	Short description of the alert
Category	High-level classification of event or KPI
Sender	Source of the alert
Sent to Groups	Groups to whom the alert has been sent
Sent	Date and time the alert was sent
Description	Additional description of the alert
Refers to Alerts	Event identifier, if the alert was caused by correlated events
Refers to KPIs	Name of the KPI, if the alert was caused by a changing KPI value

## Working with the list

From the action bar at the top of the list, you can perform the following tasks.

- To refresh the contents of the list, click **Refresh**.
- To export the contents of the list, select an **Export Option** for the list:
  - Export as HTML
  - Export all to CSV
- To print the contents of the list, select **Print Options** for the list:
  - Print all
  - Print selected
  - Print preview
- To select which columns to show, click **Configure Options** and select check boxes.
- To select which rows to show, click **Advanced Filter** to filter rows according to rules you define. Rules can be entered by column, condition, and keyword. Alternatively, enter a keyword in the quick filter field. The filter bar at the top of the list indicates if a filter has been applied and the number of rows shown relative to the total.
- To clear the filter click **Clear filter**. Alternatively, click the button on the left of the quick filter field.

A counter in the action bar at the end of the list indicates the number of items displayed and the total number of items. There is a limit of 25 to the number of items that can be displayed. If there are more rows than can be displayed at one time, you can page forward or backward by clicking the buttons in the action bar at the end of the list.

For more information about using the solution interface, click **Help** in the upper right corner of the browser page.

For more information about administering and customizing the solution, go to the IBM Intelligent Operations Center Information Center .



## Sametime Contacts

The Sametime Contacts portlet enables you to use IBM Lotus Sametime instant messaging within the IBM Intelligent Operations Center.

### What is the Sametime Contacts portlet?

The Sametime Contacts portlet provides a contacts list organized by group. It can be customized based on the people you need to communicate with. You can chat with people and modify your online status, contacts, or groups.

### What does this portlet display?

The list that appears in Sametime Contacts when you first log on depends on how your organization has set up groups in the IBM Intelligent Operations Center.

Use the drop-down menus at the top of the portlet to work with the list.

- Use the **People** menu to add contacts or modify groups.
- Use the **Options** menu to modify your status message or see only people that are online.

To get more detailed help on how to use the Sametime Contacts portlet, click the drop-down display menu in the top right corner of the portlet, and select **Help**.

---

## Operations view

Use the Operations view to maintain awareness of events. It is intended for operators, managers, or others monitoring current events and planning future events.

The Operations view is an interactive web page. It contains the following portlets, which you can think of as independent sections of the page that cooperate with one another to provide comprehensive information and interaction at the operations level:

*Table 34. Operations view portlets*

Portlet	Description
"Map" on page 114	A map of the geographical region provides event location information.  An input form selects which categories of event are shown on the map and in the Events portlet list.
"Events" on page 117	The Events portlet provides a list of events. The list contains key details for each of the events. You can display a more detailed description of an event by hovering over the row in the list.
"Coordinator - Alerts" on page 111	The Coordinator - Alerts portlet provides a dynamic, interactive list of alerts that result from changing KPIs and correlated events. The role of this portlet is to draw attention to changes in KPI or event status. The list contains key details for each of the alerts.  For example, when two severe events occur close together in location and time, an alert is sent to the Coordinator - Alerts portlet.
"Sametime Contacts"	The Sametime Contacts portlet provides a contacts list organized by group. It can be customized based on the people you need to communicate with. You can chat with people and modify your online status, contacts, or groups.

For help using each portlet, click the upper right corner of the portlet, and select **Help** from the menu displayed.

To resize a portlet, click the upper right corner of the portlet, and select options from the menu that is displayed, as follows:

- To expand the portlet to fill the page, click **Maximize**.
- To hide the portlet contents, other than its title bar, click **Minimize**.
- To restore a minimized or maximized portlet to its default view, click **Restore**.

## Map

Use the Map portlet to see where events are located on a map and to control which categories of events are shown.

### What is the Map portlet?

The Map portlet is the starting point for interaction with the Operations page. The portlet provides a visual representation of events on a map that enables you to identify location patterns, conflicts, and other issues. It can also be used to update the content of the Events portlet. You can select in the Map portlet the category of event you want to display on the map and the Events portlet list.

### What does this portlet display?

The Map portlet has two interactive interfaces as shown in the following table:

*Table 35. Map portlet display*

Interface element	Description
Map	A map of the geographical region provides event location information.
Filter	An input form selects which categories of event are shown on the map and in the Events portlet list.

Initially, when you open the Operations page, the Map portlet shows all the events that are relevant to you. The map uses the latitude and longitude values specified in the event record to show the event location in the form of an icon or a polygon outlining the area.

**Note:** If an event has no coordinates it is displayed only in the Events portlet list; it does not appear in the Map portlet.

### How is the map updated?

The map keeps you up-to-date by adding new events to the map as they enter the system, subject to any filters you set to limit the categories shown. You can display an event description by clicking the event marker on the map.

To view the filter form, click **Select content on map and event list**. The categories of event displayed on the map and in the Events portlet can be changed based upon the filter form selection that you make. The map remains beneath the filter. You can focus on the category of event you want to analyze by using the filter to hide the categories of event you do not need. The map responds to any new category selection that you submit from the filter form. When a request is submitted, the map window is updated and only the selected category event locations are plotted on the map. Change the category of events displayed by selecting or clearing a check box on the filter form. To close the filter form, click **Close content selection**. If you leave the page and return, all categories are reset to selected.

You can focus on individual events you want to analyze by ticking check boxes in the Events portlet. These events are highlighted on the map.

## Map markers

The map represents the location of an event with one of the following types of marker:

*Table 36. Map Markers*

Marker Type	Description
Icon	Pinpoint location of an event on the map with a unique icon for each category
Polygon	An outline on the map of the area associated with an event

**Note:** The icon and category name are included in details about the event in the Events portlet list. When an event is escalated to an incident in the Events portlet, the icon displayed on the map changes from a category-specific icon to a red triangle with an exclamation mark.

## Using the map controls

You can move around the map by using your mouse or keyboard.

### The map controls are on the upper left side of the map

The map controls are on the upper left side of the map. They consist of:

1. Pan arrows (up, down, left, right)
2. Zoom in
3. World view (zooms out to the maximum extent)
4. Zoom out

### Pan controls for moving around the map

To move around the map you can:

- Click and drag the map by using the mouse
- Press the up pan arrow, or the up arrow key on the keyboard, to pan north
- Press the down pan arrow, or the down arrow key on the keyboard, to pan south
- Press the right pan arrow, or the right arrow key on the keyboard, to pan east
- Press the left pan arrow, or the left arrow key on the keyboard, to pan west

### Zoom controls for magnifying or reducing the scale of the map

To zoom in and out of the map you can:

- Click the + map icon to zoom in, or the - map icon to zoom out of the center of the map
- Double-click the mouse to center the map and zoom in to the selected location
- Click the **World view** icon to maximize the zoom out to show the world view
- Press the + key on the keyboard to zoom in
- Press the - key on the keyboard to zoom out
- Press Shift while you use the mouse to draw a rectangle around the area to zoom in on

## Adding an event

You can create an event, adding it to the Map portlet map and the Events portlet list at the same time. The map and the list provide two ways of looking at the same content.

## About this task

Use the **Add Event** dialog to specify event properties, as outlined in the following table:

### Note:

Table 37. Event properties

Property	Content
Sender *	Source or user ID
Contact name	Person to contact for additional information
Contact telephone number	Contact person's telephone number
Contact e-mail address	Contact person's email address
Event type*	Event classification below category level
Event status*	Event handling instructions
Event scope*	Intended audience for the message
Restriction	Additional information required when scope is 'Restricted'
Headline*	Short description of the event
Category*	High-level event classification
Severity*	Intensity of the impact of the event
Certainty*	Confidence in the event prediction
Urgency*	Timeframe for action in response to the event
Message type	Nature of the message
Description	Additional description of the event
Web address	Web address for additional information about the event
Sent date / time*	Date and time the message was submitted or sent
Effective date / time	Date and time the message is effective
Onset date / time	Date and time the event is expected to begin
Expiration date / time	Date and time the event is expected to end
Area description	Description of the affected area
Latitude / Longitude	Coordinates of the event location

## Procedure

1. Right-click a location on the map and click **Create a new event** to launch the **Add Event** dialog. Some of the event properties are completed automatically.
2. Specify the remaining event properties, using the fields in the dialog. Properties marked with an asterisk are required for the successful creation of a new event, those properties not marked with an asterisk are optional.
3. Click **OK** to save the event or **Cancel** to stop adding the event.

## Results

An icon representing the category of the new event is displayed in the requested location on the map and its key details in the Events portlet list.

**Note:** You cannot create an event for a location on which an icon or polygon is already displayed. To create an event for a location already occupied by an event on the map, hide the event category using the filter and right-click the location again.

For more information about using the solution interface, click **Help** in the upper right corner of the browser page.

## Configuring the map

### Administrator

An administrator can alter map settings for all users. The administrator can change the center point and the zoom level for displaying the map. The administrator can also select the base map that the user sees, for example, ArcGIS.

For more information about this subject go to the IBM Intelligent Operations Center Information Center and search for configuring the map. Also, see the information center for further information about administering and customizing the solution.

## Events

Use the Events portlet to view, monitor, and manage events in the IBM Intelligent Operations Center.

### What is the Events portlet?

The Events portlet is an interactive window within the IBM Intelligent Operations Center. All events the user is authorized to see are visible on the list and on the Map portlet map. The event list can be filtered to display a subset of events.

### What does this portlet display?

The Events portlet provides a list of events. The list contains key details for each of the events. You can display a more detailed description of an event by hovering over the row in the list.

Initially, when you open the IBM Intelligent Operations Center the Events portlet shows all the events that are relevant to you. The event list automatically refreshes upon detection of a new event, or a change in an event. The categories of events shown on the Events list and on the map in the Map portlet are the same.

Remove events from both the map and list by clearing check boxes in the input form in the Map portlet. Filter the event list contents by using the filter options on the action bar at the top of the Events portlet. These filter options affect only the list and not the map.

## Event properties

The following table outlines the properties that describe an event:

*Table 38. Event properties*

Property	Content
Sender *	Source or user ID
Contact name	Person to contact for additional information
Contact telephone number	Contact person's telephone number
Contact e-mail address	Contact person's email address
Event type*	Event classification below category level
Event status*	Event handling instructions
Event scope*	Intended audience for the message
Restriction	Additional information required when scope is 'Restricted'

Table 38. Event properties (continued)

Property	Content
Headline*	Short description of the event
Category*	High-level event classification
Severity*	Intensity of the impact of the event
Certainty*	Confidence in the event prediction
Urgency*	Timeframe for action in response to the event
Message type	Nature of the message
Description	Additional description of the event
Web address	Web address for additional information about the event
Sent date / time*	Date and time the message was submitted or sent
Effective date / time	Date and time the message is effective
Onset date / time	Date and time the event is expected to begin
Expiration date / time	Date and time the event is expected to end
Area description	Description of the affected area
Latitude / Longitude	Coordinates of the event location

**Note:** Properties marked with an asterisk are required for the successful creation of a new event, those properties not marked with an asterisk are optional.

## Working with the list

From the action bar at the top of the list, you can perform the following tasks.

- To refresh the contents of the list, click **Refresh**.
- To export the contents of the list, select an **Export Option** for the list:
  - Export as HTML
  - Export all to CSV
- To print the contents of the list, select **Print Options** for the list:
  - Print all
  - Print selected
  - Print preview
- To select which columns to show, click **Configure Options** and select check boxes.
- To select which rows to show, click **Advanced Filter** to filter rows according to rules you define. Rules can be entered by column, condition, and keyword. Alternatively, enter a keyword in the quick filter field. The filter bar at the top of the list indicates if a filter has been applied and the number of rows shown relative to the total.
- To clear the filter click **Clear filter**. Alternatively, click the button on the left of the quick filter field.

A counter in the action bar at the end of the list indicates the number of items displayed and the total number of items. There is a limit of 25 to the number of items that can be displayed. If there are more rows than can be displayed at one time, you can page forward or backward by clicking the buttons in the action bar at the end of the list.

## Managing existing events

You can view or edit details for an event, change the status of an event, or cancel an event on the list.

## Procedure

1. Right-click on a row in the event list and select an option from the menu:
  - To update the information about an event, select **Update Event** to display the dialog. This results in a change in message type to update.
  - To change the event status to incident, select **Escalate to Incident**. This results in a change in the code and message type properties and a different icon on the map. When the event is an incident with an associated workflow, you can select the workflow.
  - To cancel an event, select **Cancel Event**. The event is removed from the list and the map.
  - To view the information about an event, select **Properties** to display the pop-up window.
2. Click **OK** or **Cancel**.

## Adding an event

You can create an event, adding it to the Events portlet list. When location details are provided, the event is added to the Map portlet map at the same time. There is also an option to create an event from the Map portlet. Right-click a location on the map to have the coordinates completed automatically.

## Procedure

1. Click **Add Event** to display the dialog. Many of the event properties are completed automatically. The message type is set to alert. The sent date and time can be changed.
2. Specify the remaining event properties, using fields in the dialog.
3. Click **OK** to save the event or **Cancel** to stop adding the event.

## Results

The key details for the event are included in the Events portlet list and the icon for the new event appears on the map if coordinates have been entered.

For more information about using the solution interface, click **Help** in the upper right corner of the browser page.

For more information about administering and customizing the solution go to the IBM Intelligent Operations Center Information Center.

## Coordinator - Alerts

Use the Coordinator - Alerts portlet to view your alert messages and their details.

### What is the Coordinator - Alerts portlet?

The Coordinator - Alerts portlet is an interactive window containing a list of all the current alerts relevant to you. You see only alerts that have been sent to your user groups. Alerts are notifications received when:

- Multiple events are happening in the same vicinity and at a similar time, thus might be in conflict or require coordination
- A predefined key performance indicator (KPI) value change occurs, where that change has been defined as an alert trigger by your administrator

You can also use the Coordinator - Alerts portlet to display further details of an alert.

## What does this portlet display?

The Coordinator - Alerts portlet provides a dynamic, interactive list of alerts that result from changing KPIs and correlated events. The role of this portlet is to draw attention to changes in KPI or event status. The list contains key details for each of the alerts.

To show a more detailed description of an alert, hover over the row with the cursor. To see all the information associated with that alert in a pop-up window, right-click the row and select **Properties**.

Initially, when you open the portal page, the Coordinator - Alerts portlet displays all of your current alerts. Remove any alert from the portlet by right-clicking the row and selecting **Close alert**. It is possible to close multiple alerts in this way by selecting multiple rows. Close an alert only after you have handled it appropriately because the alert is removed for all recipients when you close it.

Click the button in the upper right corner of the pop-up window to cancel it and take you back to the list.

## Alert Properties

The pop-up window for alert details displays the following properties:

*Table 39. Alert properties*

Property	Content
Headline	Short description of the alert
Category	High-level classification of event or KPI
Sender	Source of the alert
Sent to Groups	Groups to whom the alert has been sent
Sent	Date and time the alert was sent
Description	Additional description of the alert
Refers to Alerts	Event identifier, if the alert was caused by correlated events
Refers to KPIs	Name of the KPI, if the alert was caused by a changing KPI value

## Working with the list

From the action bar at the top of the list, you can perform the following tasks.

- To refresh the contents of the list, click **Refresh**.
- To export the contents of the list, select an **Export Option** for the list:
  - Export as HTML
  - Export all to CSV
- To print the contents of the list, select **Print Options** for the list:
  - Print all
  - Print selected
  - Print preview
- To select which columns to show, click **Configure Options** and select check boxes.
- To select which rows to show, click **Advanced Filter** to filter rows according to rules you define. Rules can be entered by column, condition, and keyword. Alternatively, enter a keyword in the quick filter field. The filter bar at the top of the list indicates if a filter has been applied and the number of rows shown relative to the total.
- To clear the filter click **Clear filter**. Alternatively, click the button on the left of the quick filter field.



A counter in the action bar at the end of the list indicates the number of items displayed and the total number of items. There is a limit of 25 to the number of items that can be displayed. If there are more rows than can be displayed at one time, you can page forward or backward by clicking the buttons in the action bar at the end of the list.

For more information about using the solution interface, click **Help** in the upper right corner of the browser page.

For more information about administering and customizing the solution, go to the IBM Intelligent Operations Center Information Center .

## Sametime Contacts

The Sametime Contacts portlet enables you to use IBM Lotus Sametime instant messaging within the IBM Intelligent Operations Center.

### What is the Sametime Contacts portlet?

The Sametime Contacts portlet provides a contacts list organized by group. It can be customized based on the people you need to communicate with. You can chat with people and modify your online status, contacts, or groups.

### What does this portlet display?

The list that appears in Sametime Contacts when you first log on depends on how your organization has set up groups in the IBM Intelligent Operations Center.

Use the drop-down menus at the top of the portlet to work with the list.

- Use the **People** menu to add contacts or modify groups.
- Use the **Options** menu to modify your status message or see only people that are online.

To get more detailed help on how to use the Sametime Contacts portlet, click the drop-down display menu in the top right corner of the portlet, and select **Help**.



---

## Chapter 8. Troubleshooting and support

To isolate and resolve problems with your IBM software, you can use the troubleshooting and support information, which contains instructions for using the problem-determination resources that are provided with your IBM products.

---

### Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

#### What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is “What is the problem?” This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

#### Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels

of software that are not intended to run together or have not been fully tested together.

## When does the problem occur?

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

## Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to occur for the problem to surface?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

## Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve. However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

### Related information

“Searching knowledge bases” on page 135

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

---

## Log files

To troubleshoot a problem in IBM Intelligent Operations Center, you might need to analyze log files in several systems. The following topics list the log files that are available in IBM Intelligent Operations Center, and categorize the log files by server and system.

To start the traces and view the logs, enter the commands at run time as the root user.

### Related concepts:

“Installing and using IBM Support Assistant Lite” on page 139

IBM Support Assistant Lite (ISA Lite) is a tool that collects common diagnostic data that is useful for analyzing general problems.

“Managing log files” on page 102

IBM Intelligent Operations Center stores log files in several different locations. To prevent system performance issues, periodically archive log files and remove the original log files.

### Related information:

 [Collecting Data for IBM Intelligent Operations Center V1.0](#)

## Installation management server log files

The following installation management server log files are available for troubleshooting installation issues.

Table 40. Installation management server log files

Description	Log file location
Installation log files, if installer is still running	/tmp/SL_13176/SolutionEnabler/logs
Installation log files, if installer is finished	/opt/SolutionFiles/logs/
Detailed log of all installation steps	IRU_DeploymentWizard.log
Detailed installation log of each installation task	DJT_host_nametask_nametime.log

## Portal server log files

Use the following log files to troubleshoot issues with the portal server.

When troubleshooting issues with the portal server, you might need to look at log files related to the following systems:

- WebSphere Portal
- Sametime

## Enabling tracing and viewing logs on WebSphere Portal

### About this task

WebSphere Portal logs are located at /opt/IBM/WebSphere/wp\_profile/logs/WebSphere\_Portal. Follow the steps in the procedure to start a trace and view a log.

### Procedure

1. Log in to the WebSphere Application Server administrative console.
2. Click **Troubleshooting > Logs and Trace**.
3. Click **WebSphere\_Portal > Change log level details**.
4. Click the Runtime tab and paste in the following command: `*=info: com.ibm.iss.*=all: com.ibm.ioc.*=all`
5. Click **OK**.

6. To view a log, enter the following commands:  

```
cd /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal
tail -f trace.log
```

## Enabling tracing and viewing logs on Sametime

### About this task

Sametime logs are located at `/tmp/domino.log` and `/local/notesdata/trace/Sametime_date.log`. Follow the steps in the procedure to enable tracing and view the logs.

### Procedure

1. For `/tmp/domino.log`, enter the following command: `tail -f /tmp/domino.log`
2. For `/local/notesdata/trace/Sametime_date.log`, enter the following command: `tail -f /local/notesdata/trace/Sametime_date.log`, where *date* is the date for which the log is required.

## Application and integration server log files

Use the following log files to troubleshoot issues with the application and integration server.

When troubleshooting issues with the application and integration server, you might need to look at log files related to the following systems:

- Model manager - application and integration server
- Model manager - portal server
- WebSphere MQ and WebSphere Message Broker

## Enabling tracing and viewing logs for model manager on the application and integration server

### About this task

Logs for model manager on the application and integration server are located at `/opt/IBM/WebSphere/AppServer/profiles/MIHCustom01/logs/MIH_MEMBER01/`. Follow the steps in the procedure to start a trace and view a log.

### Procedure

1. Log in to the WebSphere Application Server administrative console at `http://app_integ_server:9063/admin`.
2. Click **Troubleshooting > Logs and Trace**.
3. Click **MIH MEMBER01 > Change log level details**.
4. Click the **Runtime** tab.
5. Change the log detail levels for the diagnostic trace to `*=info:com.ibm.iss.iic.=all`.
6. Click **server1 > Diagnostic Trace**.
7. Click the **Runtime** tab.
8. Increase the value of the **Maximum File Size** to 100 MB.

## Enabling tracing and viewing logs for model manager on the portal server

### About this task

Logs for model manager on the portal server are located at `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal`. Use the procedure to start a trace and view a log.

### Procedure

Enable IBM Intelligent Operations Center portal server logging for the model manager service.

Enter the following command:

```
*=info:com.ibm.iss.common.logger.core.modelmanager.ModelManagerLogger=finest
```

## Enabling tracing and viewing logs for WebSphere MQ and WebSphere Message Broker

### About this task

Logs for WebSphere MQ and WebSphere Message Broker are stored at the following locations:

- /var/mqm/errors
- /var/mqm/qmgrs/IOC!MB!QM/errors

Trace files are written to the /var/mqm/trace directory. You can turn on tracing for a single queue manager or all queue managers, as shown in the following procedure.

### Procedure

1. To start, end, or format a trace, choose the appropriate command:
  - To start a trace for all processes, enter the following command: `strmqtrc -e`
  - To start a trace for the IBM Intelligent Operations Center queue manager, enter the following command: `strmqtrc -m IOC.MB.QM`
  - To start a high detail trace for the IBM Intelligent Operations Center queue manager, enter the following command: `strmqtrc -t all -t detail -m IOC.MB.QM`
  - To end all tracing, enter the following command: `endmqtrc -a`
  - To format the binary trace files in ASCII format, enter the following command: `dspmqtrc *.TRC`
2. To check the status of WebSphere Message Broker:
  - a. Enter the following command: `ps -ef | grep IOC_BROKER`
  - b. Check the status of the following processes:
    - `bipservice IOC_BROKER`
    - `bipbroker IOC_BROKER`
    - `biphttplistener IOC_BROKER`
    - `DataFlowEngine IOC_BROKER 5fe69373-2f01-0000-0080-9ab9c3579b15 default`

## Analytic server log files

Use the following log files to troubleshoot issues with the analytic server.

When troubleshooting issues with the analytic server, you might need to look at log files related to IBM WebSphere Business Monitor.

## Enabling tracing and viewing logs for IBM WebSphere Business Monitor on the analytic server

### About this task

Logs for IBM WebSphere Business Monitor on the analytic server are located at /opt/IBM/WebSphere/AppServer/profiles/qmwas/logs/server1. Follow the steps in the procedure to start a trace and view a log.

### Procedure

1. Log in to the WebSphere Application Server administrative console.
2. Click **Troubleshooting > Logs and Trace**.
3. Click **server1 > Change log level details**.

4. Click the Runtime tab and paste in the following trace level code: `*=info: com.ibm.wbm.*=finest:  
com.ibm.events.*=all: com.ibm.wbimonitor.xsp.cei.*=all:  
com.ibm.wbimonitor.xsp.eventselector.*=all`
5. Click **OK**.

## Event and management server log files

Use the following log files to troubleshoot issues with the event and management server.

When troubleshooting issues with the event and management server, you might need to look at log files related to the following systems:

- Tivoli Netcool/OMNIBus XML probe
- Tivoli Netcool/OMNIBus (object server) database
- Tivoli Netcool/OMNIBus (Process Agent) Database
- Tivoli Netcool/Impact

**Related information:**

 [IBM WebSphere Portal 7 Product Documentation](#)

## Enabling tracing and viewing logs for the Tivoli Netcool/OMNIBus XML probe

### About this task

WebSphere Portal logs are located at `/opt/IBM/netcool/omnibus/log/ioc_xml.log`. Follow the steps in the procedure to start a trace and view a log.

### Procedure

1. Open a terminal on the event and management server.
2. Enter the following command: `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`
3. If the Connection status OK message is not displayed at the bottom of the file, to rename the current log file, enter the following command: `mv /opt/IBM/netcool/omnibus/log/ioc_xml.log /opt/IBM/netcool/omnibus/log/old_ioc_xml.log`
4. If the Connection status OK message is not displayed, you might also see the message Probe shutting down. To restart the probe, enter the following command:  

```
cd /opt/IBM/netcool/omnibus/probes/  
./ncp_xml -name ioc_xml -propsfile linux2x86/ioc_xml.props &
```
5. After approximately 1 minute, enter the following command again: `tail -f /opt/IBM/netcool/omnibus/log/ioc_xml.log`
6. If the Connection status OK message is still not displayed, check the `/opt/IBM/netcool/omnibus/log/ioc_xml.log` file for errors. A connection problem might mean that the object server is down. See the following section, *Enabling tracing and viewing logs for the Tivoli Netcool/OMNIBus (object server) database*.

## Enabling tracing and viewing logs for the Tivoli Netcool/OMNIBus (object server) database

### About this task

The log files are located at the following locations:

- `/opt/IBM/netcool/omnibus/log/ioc_xml.log`
- `/opt/IBM/netcool/omnibus/log/NCOMS*.*`, for example:
  - `/opt/IBM/netcool/omnibus/log/NCOMS.log`
  - `/opt/IBM/netcool/omnibus/log/NCOMS_trigger_stats.log1`
  - `/opt/IBM/netcool/omnibus/log/NCOMS_profiler_report.log1`



Follow the steps in the procedure to start a trace and view a log.

## Procedure

1. Log in to a terminal as a root user.
2. Enter the following command: `/opt/IBM/netcool/omnibus/bin/nco_config &`
3. If you are asked do you want to import from `omni.dat`, click **yes**, and then click **finish**.
4. Minimize the process agent window.
5. Right-click **NCOMs**.
6. Choose the appropriate option:
  - If the **Connect As...** option is not displayed, you must start the NCOMS object server:
    - a. To start the NCOMS object server, close `nco_config` and enter the following command:  
`/opt/IBM/netcool/omnibus/bin/nco_objserv -name NCOMS &`
    - b. If the NCOMS object server does not start, look for a `NCOMS.pid` file in the `/opt/IBM/netcool/omnibus/var` directory and delete it, then try to start the server again.
  - If the **Connect As...** option is displayed, click **Connect As...**, then for user name, enter `root`, and enter the password.
7. Once you have started the NCOMs server, to restart the probe, enter the following command:  
`cd /opt/IBM/netcool/omnibus/probes/  
./nco_p_xml -name ioc_xml -propsfile linux2x86/ioc_xml.props &`
8. To view the log file, enter the following command: `tail -f /opt/IBM/netcool/omnibus/log/NCOMS.log`

## Tivoli Netcool/OMNIBus (Process Agent) Database

The Tivoli Netcool/OMNIBus (Process Agent) Database log file is located at `/opt/IBM/netcool/omnibus/log/NCO_PA.log`.

## Tivoli Netcool/Impact

### About this task

The log file is located at `opt/IBM/netcool/impact/log/`. Follow the steps in the procedure to start a trace and view a log.

## Procedure

1. Log in to the Tivoli Netcool/Impact administrative console at `http://localhost:9085/nci/main` with the user name `admin` and the password. If a login prompt is not displayed, enter the following commands in a terminal window:  
`su - netcool  
/opt/IBM/netcool/bin/ewas.sh start`
2. In the Service Status window, scroll down and make sure that the following services are running, as indicated by a green symbol:
  - `IOC_CAP_Event_Reader`
  - `IOC_Notification_Reader`
3. Also in the Service Status window, click the **View Log** icon next to **PolicyLogger** to see if there are any errors displayed in the log.
4. If there are one or more errors in the log, for more details see the log files in the following directory:  
`/opt/IBM/netcool/impact/log/`
5. If you need more details, set the log levels higher. Click **PolicyLogger**, and then set the value of **Highest log level** to 3 and select the appropriate check boxes.

## What to do next

You can turn on various logs at run time through the WebSphere Application Server administrative console. For more information about turning on portal tracing and other traces that are available from WebSphere Portal, see the link near the start of the topic for the WebSphere Portal product documentation and search for *Logging and tracing*.

## Summary of systems and log file locations

The following table lists the log file locations for each of the systems contained in IBM Intelligent Operations Center. All the log files are created automatically. View them using the appropriate tail commands.

Table 41. IBM Intelligent Operations Center systems and log file locations

System	Logs
IBM Cognos Business Intelligence	/opt/IBM/WebSphere/AppServer/profiles/CognosAppSrv01/logs/CognosX_GW/*.log  /opt/IBM/WebSphere/AppServer/profiles/CognosAppSrv01/logs/CognosX_Dispatch/*.log  /opt/IBM/WebSphere/AppServer/profiles/CognosAppSrv01/logs/server1/*.log
DB2	/home/db2inst1/sqllib/log/db2start/*.log  /home/db2inst1/sqllib/log/instance.log
IBM HTTP Server	/opt/IBM/HTTPServer/logs/*.log
IBM Tivoli Monitoring	/opt/IBM/ITM/logs/*.log
IBM Integrated Information Core model manager	/opt/IBM/WebSphere/AppServer/profiles/MIHDMgr01/logs/dmgr/*.log  /opt/IBM/WebSphere/AppServer/profiles/MIHCustom01/logs/MIH_MEMBER01/*.log
Lotus Sametime Community Server / Lotus Domino Server	/tmp/domino.log
Tivoli Netcool/Impact	/opt/IBM/netcool/log/create_new_server.log  /opt/IBM/netcool/eWAS/installEWAS.log  /opt/IBM/netcool/impact/log/*.log  /opt/IBM/netcool/eWAS/logs/manageprofiles/ImpactProfile/*.log
Tivoli Netcool/OMNIBus	/opt/IBM/netcool/*.log  /opt/IBM/netcool/omnibus/log/*.*
WebSphere Portal	/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/*.log  /opt/IBM/WebSphere/wp_profile/logs/server1/*.log
WebSEAL	/var/pdweb/log/*.log
WebSphere Application Server	/opt/IBM/WebSphere/AppServer/profiles/\${profile_name}/logs/\${server_name}/*.log

Table 41. IBM Intelligent Operations Center systems and log file locations (continued)

System	Logs
IBM WebSphere Business Monitor	<p>/opt/IBM/WebSphere/AppServer/logs/wbm/install/*.log</p> <p>/opt/IBM/WebSphere/AppServer/logs/wbm/install.FP7003/*.log</p> <p>/opt/IBM/WebSphere/AppServer/logs/xml/update/*.log</p> <p>/opt/IBM/WebSphere/AppServer/logs/xml/update.FP1007/*.log</p> <p>/opt/IBM/WebSphere/AppServer/profiles/qmwas/logs/server1/*.log</p>
WebSphere Message Broker	Logs are not enabled by default. For information on enabling the logs, see the WebSphere Message Broker information center.
WebSphere MQ	<p>/var/mqm/errors/AMQERR*.log</p> <p>/var/mqm/qmgrs/IOC!MB!QM/errors/AMQERR*.log</p>
Tivoli Access Manager	/var/PolicyDirector/log/*.log
Tivoli Directory Server	/var/idsldap/V6.2/*.log
Tivoli Identity Manager	/opt/IBM/WAS/V6.1/profiles/ISPAAppSrv01/logs/server1/*.log

## IBM Intelligent Operations Center Messages

Each message topic helps you to identify the cause of a particular error condition in the IBM Intelligent Operations Center and recommends actions to take to resolve the error.

To help you understand the errors that you might encounter while using IBM Intelligent Operations Center, each message topic is divided into three sections: the message that is displayed in the IBM Intelligent Operations Center or its logs, an explanation, and an action.

### The message

Contains two identifiers, which are the error identification and associated text. The error identification is the message ID. It is a unique number that identifies a message. A final character of E indicates that the message resulted from an error, W indicates a warning message, and I indicates an information message.

### The explanation

Contains an additional explanation of the message.

### The user response

Suggests the corrective action for resolving the error.

To help you search for information about an error message, enter the ID number of the error message in the Search field in the information center.

**Note:** The topics in this section contain only messages that are specific to IBM Intelligent Operations Center. For all other messages, see the product documentation.

## CHK: Installation prerequisite checking messages

Use the information in this section to understand and respond to error, warning, and informational messages generated during the installation prerequisite checking process.

### Related tasks:

“Checking installation prerequisites” on page 19

During the installation of IBM Intelligent Operations Center, errors or warnings might be displayed if the prerequisites are not met on all of the six target servers. Run the installation prerequisites checking tool to verify that the installation prerequisites are satisfied.

“Installing the fix pack” on page 41

Use the command line to install the IBM Intelligent Operations Center 1.0 Fix Pack 1.

“Restarting a failed installation for the fix pack” on page 42

If the IBM Intelligent Operations Center 1.0 Fix Pack 1 installation fails, resolve the issue and check the status of the components installed before restarting the installation.

---

**CHK001E** RPM package *xxx* is not installed on server *yyy*.

**Explanation:** The indicated RPM package is not installed on the indicated server.

**User response:** Install the missing Red Hat Package Manager package. For more detail on installing dependencies, see the link at the end of the topic.

### Related tasks:

“Extracting installation files and installing dependencies” on page 18

After copying the required files to a temporary location, extract the installation files. Then install the dependencies before deploying the IBM Intelligent Operations Center.

---

**CHK002W** Disk space is not enough on server *xxx*.

**Explanation:** There is insufficient disk space on the indicated server.

**User response:** Ensure that 30 GB disk space is available in both the /tmp and the /opt directories, so that a total of 60 GB disk space is available on the server.

---

**CHK003W** Memory size is less than *xxx* GB on server *yyy*.

**Explanation:** There is insufficient memory available on the indicated server.

**User response:** Ensure that the memory size of the server is more than *xxx*.

---

**CHK004W** Directory *xxx* already exists on server *yyy*.

**Explanation:** The indicated directory already exists on the target server. The directory cannot exist on the target server.

**User response:** Ensure that the directory *xxx* does not already exist on the target server.

---

**CHK005E** Port *xxx* already in use on server *yyy*.

**Explanation:** The indicated port is already in use on the target server.

**User response:** Ensure that port number *xxx* is not already in use on the target server.

---

**CHK006E** Host name is not *xxx* on server *yyy*.

**Explanation:** An incorrect host name was specified.

**User response:** Ensure that the host name is set correctly on the target server. The value of the host name must be the same as the value you specified in the precheck.properties file.

---

**CHK007E** Network connection is broken from *xxx* to *yyy*.

**Explanation:** The host name could not be reached from the indicated server.

**User response:** Ping *yyy* from server *xxx* using the fully-qualified host name.

---

**CHK008E** SELinux is running on server *xxx*.

**Explanation:** SELinux cannot be running on the target server.

**User response:** Shut down SELinux on the target server.

---

**CHK009E** Firewall is running on server *xxx*.

**Explanation:** A firewall cannot be running on the target server.

**User response:** Shut down the firewall on the target server. Enter the following command: `service iptables stop`

---

**CHK010W** Cannot look up host name or IP from DNS for server *xxx*.

**Explanation:** The host name or IP address cannot be determined.

**User response:** If the DNS server is configured for target server *xxx*, make sure that the host name returned by the command `nslookup IP` is the same as the host name returned by the `hostname -f` command. Note that the host name is case-sensitive. Also, the IP address returned by the `nslookup hostname` command must be the same as the IP address returned by the `hostname -i` command. For more details on the use of DNS, see the link at the end of the topic.

**Related tasks:**

“Preparing the servers” on page 16  
Before you begin the installation, first prepare the servers that the IBM Intelligent Operations Center will be installed on.

---

**CHK011W Max number of open files is less than 10000 on server *xxx*.**

**Explanation:** The limit of the maximum number of open files is set to too low a value.

**User response:** Ensure that the maximum open files limit is more than 10000. To solve the problem, add to the file `/etc/security/limits.conf` the following two lines:

```
* hard nfile 12000
* soft nfile 12000
```

Then enter the command `ldconfig`.

---

**CHK012E Linux release is not *xxx*.**

**Explanation:** The operating system is not the supported level.

**User response:** Ensure that the operating system release is Red Hat Enterprise Linux 5 Update 5.

---

**CHK013E Linux distribution is not *xxx*.**

**Explanation:** The Linux distribution is incorrect.

**User response:** Ensure that the Linux distribution is RedHatEnterpriseServer. To check the Linux distribution, enter the following command: `lsb_release -a`

---

**CHK014E WebSphere Application Server profile *xxx* is not started, or account or password is invalid on server *yyy*.**

**Explanation:** The system is unable to access the WebSphere Application Server profile.

**User response:** Make sure that Tivoli Directory Server is started on the event and management server and that WebSphere Application Server profile *xxx* is started on server *yyy*. Also, make sure that the administration password of this profile is updated according to the

password guidelines, see the link at the end of the topic. The password must be changed both within the Tivoli Directory Server and the `updateProperty.sh` script file.

**Related information:**

 [PO00017 Fix Download](#)

---

**CHK015E Password policy needs to be changed on server *xxx*.**

**Explanation:** The password policy needs to be changed.

**User response:** Edit `/etc/pam.d/system-auth` to change the password policy. For more detail on modifying the password policy before installation, see the link at the end of the topic.

**Related information:**

 [Modifying the password policy before installation](#)

---

**CHK016E IPv6 is not enabled on server *xxx*.**

**Explanation:** The required internet protocol is not enabled on the indicated server.

**User response:** Enable Internet Protocol Version 6 (IPV6) on the target server.

---

**CHK018E Users are not allowed to connect to *xxx* via SSH**

**Explanation:** Users cannot connect to the specified server.

**User response:** Edit the `/etc/ssh/sshd_config` file on the target server so that all root and other users can log on to it by using SSH. For more detail, see the link at the end of the topic.

**Related tasks:**

“Preparing the servers” on page 16  
Before you begin the installation, first prepare the servers that the IBM Intelligent Operations Center will be installed on.

---

**CHK019E *xxx* is a soft link on server.**

**Explanation:** The indicated directory is a soft link to another directory.

**User response:** Ensure that the directory *xxx* is not a soft link to another directory. For more detail, see the link at the end of the topic.

**Related tasks:**

“Preparing the servers” on page 16  
Before you begin the installation, first prepare the servers that the IBM Intelligent Operations Center will be installed on.

---

**CHK020E** Tivoli Directory Server instance *xxx* is not started on server

**Explanation:** Tivoli Directory Server needs to be started on the target server.

**User response:** Ensure the Tivoli Directory Server instance *xxx* is started on the target server.

---

**CHK021E** DB2 instance *xxx* is not started on server *yyy*.

**Explanation:** The indicated DB2 instance is not started on the target server.

**User response:** Ensure the DB2 instance *xxx* is started on the target server.

---

**CHK022E** WebSphere Application Server *xxx* is not started on server *yyy*.

**Explanation:** The indicated WebSphere Application Server is not started on the target server.

**User response:** Ensure the WebSphere Application Server *xxx* is started on the target server.

---

**CHK023E** 'localhost' is not mapped to 127.0.0.1 on server *yyy*.

**Explanation:** The local host is not mapped to the correct IP address on the indicated server.

**User response:** Ensure localhost is mapped to 127.0.0.1 in the /etc/hosts file on the target server.

---

**CHK404E** OS type of target server *xxx* is not *yyy*.

**Explanation:** The operating system of the target server is not supported.

**User response:** Ensure that the operating system of the target server is Red Hat Enterprise Linux.

---

**CHK405E** OS bit of target server *xxx* is not *yyy*.

**Explanation:** The operating system of the target server is not supported.

**User response:** Ensure that the target server has a 64-bit operating system.

---

**CHK406E** CPU of target server *xxx* is not *yyy*.

**Explanation:** The CPU of the target server is not supported.

**User response:** Ensure that the CPU of the target server is EM64T or AMD64.

---

**CHK408E** Cannot connect to server *xxx* because of wrong host name, account or password.

**Explanation:** An incorrect host name, account, or password was provided.

**User response:** Ensure that the SSH service is open on the target server, and ensure that the account name and password are in the precheck.properties file.

---

**CHK409E** Time or time zone is not synchronized between *xxx* and *yyy*.

**Explanation:** The time zone and date time are not the same across the servers.

**User response:** Ensure that the time zone and data time are identical across all target servers and the installation server.

---

**CHK420E** Value is not provided for key *xxx* in properties file.

**Explanation:** A value for the indicated key is not specified.

**User response:** Ensure that a value is provided for key *xxx* in the precheck.properties file.

---

**CHK421E** Account for server *xxx* is not root account.

**Explanation:** An incorrect account is specified for the indicated server.

**User response:** Ensure the account provided in the precheck.properties file is root.

---

**CHK424E** Value *xxx* for key *yyy* is not valid, it should be "EM64T" or "AMD64".

**Explanation:** An incorrect value was specified for the indicated key.

**User response:** Ensure that the value for key *xxx* is EM64T or AMD64.

---

**CHK425E** Value *xxx* for key *yyy* is not a valid host name.

**Explanation:** An incorrect value was specified for the indicated key.

**User response:** Ensure that the value for key *yyy* is a valid, fully-qualified host name.

---

## Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

### About this task

You can find useful information by searching the information center for IBM Intelligent Operations Center, but sometimes you need to look beyond the information center to answer your questions or resolve problems.

### Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

- Search for content by using the IBM Support Assistant (ISA) Lite.  
ISA Lite is a no-charge software tool that helps you answer questions and resolve problems with IBM software products. For instructions for downloading and installing ISA Lite, see the links at the end of the topic.
- Find the content that you need by using the IBM Support Portal.  
The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos ([https://www.ibm.com/blogs/SPNA/entry/the\\_ibm\\_support\\_portal\\_videos](https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos)) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.
- Search for content about IBM Intelligent Operations Center by using one of the following additional technical resources:
  - IBM Intelligent Operations Center technotes and APARs (problem reports)
  - IBM Intelligent Operations Center Support Portal page
  - IBM Intelligent Operations Center Forums and communities page
- Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any [ibm.com](https://www.ibm.com)® page.
- Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to include information that is outside the [ibm.com](https://www.ibm.com) domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on [ibm.com](https://www.ibm.com).

**Tip:** Include “IBM” and the name of the product in your search if you are looking for information about an IBM product.

**Related concepts:**

“Installing and using IBM Support Assistant Lite” on page 139

IBM Support Assistant Lite (ISA Lite) is a tool that collects common diagnostic data that is useful for analyzing general problems.

“Intelligent Operations Center - About” on page 97

Use the Intelligent Operations Center - About portlet to view details of the version of the IBM Intelligent Operations Center and the integrated IBM Smarter Cities Software Solutions that you have installed.

**Related information:**

 [Downloading IBM Support Assistant Lite for IBM Intelligent Operations Center 1.0](#)

---

## Getting fixes from Fix Central

You can use Fix Central to find the fixes that are recommended by IBM Support for various products, including IBM Intelligent Operations Center. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. An IBM Intelligent Operations Center product fix might be available to resolve your problem.

**Procedure**

To find and install fixes:

1. Obtain the tools that are required to get the fix. If it is not installed, obtain your product update installer. You can download the installer from Fix Central. This site provides download, installation, and configuration instructions for the update installer.
2. Select IBM Intelligent Operations Center as the product, and select one or more check boxes that are relevant to the problem that you want to resolve.
3. Identify and select the fix that is required.
4. Download the fix.
  - a. Open the download document and follow the link in the “Download Package” section.
  - b. When downloading the file, ensure that the name of the maintenance file is not changed. This change might be intentional, or it might be an inadvertent change that is caused by certain web browsers or download utilities.
5. To apply the fix, follow the instructions in the “Installation Instructions” section of the download document.
6. Optional: Subscribe to receive weekly email notifications about fixes and other IBM Support updates.

**Related tasks:**

“Subscribing to support updates” on page 139

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

**Related information:**

 [Fix Central help](#)

---

## Contacting IBM Support

IBM Support provides assistance with product defects, answering FAQs, and performing rediscovery.

**Before you begin**

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For



information about the types of available support, see the Support portfolio topic in the *Software Support Handbook*.

## Procedure

Complete the following steps to contact IBM Support with a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information. For information on using IBM Support Assistant Lite to collect IBM Intelligent Operations Center log files, see the links at the end of the topic.
3. Submit the problem to IBM Support in one of the following ways:
  - Using IBM Support Assistant (ISA) Lite. See the links at the end of the topic.
  - Online through the IBM Intelligent Operations Center Support Portal page: You can open, update, and view all your Service Requests from the Service Request portlet on the Service Request page.
  - By phone: For the phone number to call in your region, see the Directory of worldwide contacts web page.

## Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

## What to do next

Be prepared to work with the IBM technical-support representative by using IBM Assist On-Site, which is a remote-assistance plug-in that you can download to your computer. The IBM technical-support representative can use IBM Assist On-Site to view your desktop and share control of your mouse and keyboard. This tool can shorten the time that it takes to identify the problem, collect the necessary data, and solve the problem. For more information, see IBM Assist On-Site.

### Related concepts:

“Installing and using IBM Support Assistant Lite” on page 139

IBM Support Assistant Lite (ISA Lite) is a tool that collects common diagnostic data that is useful for analyzing general problems.

“Intelligent Operations Center - About” on page 97

Use the Intelligent Operations Center - About portlet to view details of the version of the IBM Intelligent Operations Center and the integrated IBM Smarter Cities Software Solutions that you have installed.

### Related information:



Downloading IBM Support Assistant Lite for IBM Intelligent Operations Center 1.0

---

## Exchanging information with IBM

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

### Related concepts:

“Installing and using IBM Support Assistant Lite” on page 139

IBM Support Assistant Lite (ISA Lite) is a tool that collects common diagnostic data that is useful for analyzing general problems.

### Related information:

 Downloading IBM Support Assistant Lite for IBM Intelligent Operations Center 1.0

## Sending information to IBM Support

To reduce the time that it takes to resolve your problem, you can send trace and diagnostic information to IBM Support.

### Procedure

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR) using The Service Request tool.
2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data automatically or manually:
  - Collect the data automatically using IBM Support Assistant (ISA) Lite. See the links near the beginning of the topic.
  - Collect the data manually. For information about IBM Intelligent Operations Center log files, see the links near the beginning of the topic.
3. Compress the files by using the ZIP or TAR format.
4. Transfer the files to IBM. You can use one of the following methods to transfer the files to IBM:
  - The Service Request tool
  - Standard data upload methods: FTP, HTTP
  - Secure data upload methods: FTPS, SFTP, HTTPS
  - Email

All of these data exchange methods are explained on the IBM Support site.

## Receiving information from IBM Support

Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

### Before you begin

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

### Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as anonymous. Use your email address as the password.
2. Change to the appropriate directory:
  - a. Change to the /fromibm directory.  
`cd fromibm`
  - b. Change to the directory that your IBM technical-support representative provided.  
`cd nameofdirectory`
3. Enable binary mode for your session.

- binary
4. Use the **get** command to download the file that your IBM technical-support representative specified.  
`get filename.extension`
  5. End your FTP session.  
`quit`

---

## Installing and using IBM Support Assistant Lite

IBM Support Assistant Lite (ISA Lite) is a tool that collects common diagnostic data that is useful for analyzing general problems.

ISA Lite gathers the following types of information:

- Platform problem determination files
- System log and trace files
- Platform provisioning files
- System configuration files
- Java™ dump files
- Problem determination framework internal log files

To download ISA Lite for IBM Intelligent Operations Center 1.0, see the link at the end of the topic.

To install and use ISA Lite, follow the instructions in the Quick Start Guide included in the download package.

### Log files collected by ISA Lite

ISA Lite for IBM Intelligent Operations Center 1.0 collects many log files. For more information about the log files that ISA Lite collects, see the link at the end of the topic to the Log files section.

#### Related concepts:

“Log files” on page 125

To troubleshoot a problem in IBM Intelligent Operations Center, you might need to analyze log files in several systems. The following topics list the log files that are available in IBM Intelligent Operations Center, and categorize the log files by server and system.

#### Related information:

 [Downloading IBM Support Assistant Lite for IBM Intelligent Operations Center 1.0](#)

---

## Subscribing to support updates

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

### About this task

By subscribing to receive updates, you can receive important technical information and updates for specific IBM Support tools and resources. You can subscribe to updates by using one of two approaches:

#### RSS feeds

The following RSS feed is available for IBM Intelligent Operations Center: *IBM Intelligent Operations Center*.

For general information about RSS, including steps for getting started and a list of RSS-enabled IBM web pages, visit the IBM Software Support RSS feeds site.

## My Notifications

With My Notifications, you can subscribe to Support updates for any IBM product. (My Notifications replaces My Support, which is a similar tool that you might have used in the past.) With My Notifications, you can specify that you want to receive daily or weekly email announcements. You can specify what type of information you want to receive (such as publications, hints and tips, product flashes (also known as alerts), downloads, and drivers). My Notifications enables you to customize and categorize the products about which you want to be informed and the delivery methods that best suit your needs.

## Procedure

To subscribe to Support updates:

1. To subscribe to the *IBM Intelligent Operations Center* RSS feed, use the following substeps:
  - a. Open the link *IBM Intelligent Operations Center* RSS feed.
  - b. In the *Subscribe with Live Bookmark* window, select a folder in which to save the RSS feed bookmark and click **Subscribe**.

For more information on subscribing to RSS feeds, see the *IBM Software Support RSS feeds* link in the *Related information* section at the end of the topic.

2. To subscribe to My Notifications, go to the *IBM Support Portal* and click **My Notifications** in the **Notifications** portlet.
3. Sign in using your IBM ID and password, and click **Submit**.
4. Identify what and how you want to receive updates.
  - a. Click the **Subscribe** tab.
  - b. Select *IBM Intelligent Operations Center* and click **Continue**.
  - c. Select your preferences for how to receive updates, whether by email, online in a designated folder, or as an RSS or Atom feed.
  - d. Select the types of documentation updates that you want to receive, for example, new information about product downloads and discussion group comments.
  - e. Click **Submit**.

## Results





Until you modify your RSS feeds and My Notifications preferences, you receive notifications of updates that you have requested. You can modify your preferences when needed (for example, if you stop using one product and begin using another product).

### Related tasks:

“Getting fixes from Fix Central” on page 136

You can use Fix Central to find the fixes that are recommended by IBM Support for various products, including *IBM Intelligent Operations Center*. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. An *IBM Intelligent Operations Center* product fix might be available to resolve your problem.

### Related information

-  [IBM Software Support RSS feeds](#)
-  [Subscribe to My Notifications support content updates](#)
-  [My notifications for IBM technical support](#)
-  [My notifications for IBM technical support overview](#)

---

## Troubleshooting tips

This section contains a list of commonly occurring problems and some troubleshooting tips for each item.

### Working with Sametime portlet causes other portlets to reload

In the Sametime portlet, if you are working with contacts, clicking the People or Options menu causes all the other portlets to reload. To avoid being distracted by the activity in the other portlets, maximize the Sametime portlet while you are working with it. While the Sametime portlet is maximized, the other portlets are still reloaded but the activity is hidden from view.

### Key performance indicator processing stops after a period

In the IBM Intelligent Operations Center, key performance indicator (KPI) processing occasionally stops after a period, for example, overnight. For information about resolving the problem, see the link at the end of the topic to the *Key performance indicator processing stops after a period of time* troubleshooting technote.

Fix Pack 1

### Troubleshooting fix pack installation problems

There is an automatic prerequisite check included in the IBM Intelligent Operations Center 1.0 installation script where the script first checks installation prerequisites. Any errors detected during the installation are displayed and written to a fix pack log file. Use the option to stop, if there is a serious problem. Check and resolve the issue before continuing with the fix pack installation. See the related concept link at the end of the topic for information about how to do this.

Fix Pack 1

### Installing other solutions with the fix pack

If you are installing another solution with the IBM Intelligent Operations Center 1.0 Fix Pack 1, you must disable the heartbeat service and you might need to stop server monitoring. See the related task links at the end of the topic for details on how to complete these tasks.

### IOControl command not running

There can only one user session running an **IOControl** command at any one time. To check whether there is already another process running, run the command `ps -ef | grep /ISP/mgmt/`. The output indicates if another process is running, for example:

```
root 5597 5590 32 17:52 pts/2 00:00:05 /opt/ibm/java2-i386-50/jre/bin/java -classpath /opt/IBM/ISP/mgmt
/scripts/./apache-ant-1.8.1/lib/ant-launcher.jar -Dant.home=/opt/IBM/ISP/mgmt/scripts/./apache-ant-1.8.1
-Dant.library.dir=/opt/IBM/ISP/mgmt/scripts/./apache-ant-1.8.1/lib org.apache.tools.ant.launch.Launcher
-cp -DCmdPassword password -DICP.action status all
root 5962 29184 0 17:52 pts/1 00:00:00 grep /ISP/mgmt/
```

In this example you can use the `kill -9 5597` command to end the process.

**Note:** If you change passwords, ensure that you follow the password guidelines, see the related information link at the end of the topic.

### IOControl command query not returning results

When you run the **IOControl** command status query on all the servers, the required status is not displayed. The result might be a partial server list or none at all. In both cases, a message indicates that the command completed successfully. To resolve this issue go to the `/opt/IBM/ISP/logs` folder and delete `status.log`.

## Related tasks:

"Installing the fix pack" on page 41

Use the command line to install the IBM Intelligent Operations Center 1.0 Fix Pack 1.

"Restarting a failed installation for the fix pack" on page 42

If the IBM Intelligent Operations Center 1.0 Fix Pack 1 installation fails, resolve the issue and check the status of the components installed before restarting the installation.

"Managing the heartbeat service" on page 101

The heartbeat service provided with the IBM Intelligent Operations Center 1.0 Fix Pack 1 restarts middleware components if they fail.

"Starting and stopping server monitoring" on page 100

You can start or stop each Tivoli Enterprise Monitoring Agent if required because of performance or other concerns.

## Related information:

 Key performance indicator processing stops after a period of time troubleshooting technote

 Password documentation

---

## Restarting a failed installation for the fix pack

### Fix Pack 1

If the IBM Intelligent Operations Center 1.0 Fix Pack 1 installation fails, resolve the issue and check the status of the components installed before restarting the installation.

## Before you begin

There is an automatic prerequisite check included in the fix pack installation script where the script first checks installation prerequisites. Any errors detected during the installation are displayed and written to a fix pack log file: `preCheck_Topology_ioc_topo_date.log`. See the related concept link at the end of the topic for details of messages. Select the option to stop, if there is a serious problem. Check and resolve the issue before restarting the fix pack installation.

## About this task

If the fix pack installation fails, the status of some middleware components is set to "Uncertain" in the topology model file, `/fixpack/ioc/topology/ioc_topo.xml`. Before you resume the installation, complete the procedure. If the installation of a component fails, remove the partially-installed component. Fix the problem that caused the installation failure. Then rerun fix pack installation, so that the component is fully installed.

## Procedure

1. On the installation management server, navigate to the topology model file, `/ioc/topology/ioc_topo.xml`. The path is within the fix pack folder where fix pack package is extracted.
2. Search the topology model file and find all components with "Uncertain" status. Process each one of these components according to the following steps. An example of the lines identifying such a component is as follows:

```
<component version="7.0.1.7" status="Uncertain" id="mq_fixpack" type="mq_fixpack" package="WMBQ">
<connection id="mqbase" role="mq_base"/>
</component>
```
3. To check the installation status of the component, on the target server where the middleware is being installed, check this file: `/tmp/ioc/script/ioc_topo/component_id/UUID.res`. If the file contains 0, the installation is successful, otherwise the installation failed.
  - a. If the component is installed successfully, complete step 4 before you restart the installation.

- b. If the component is not installed, before you restart the installation remove the partially installed middleware according to the documentation provided for that component .
4. In the topology model file, search for "Uncertain".
5. Change the status attribute of the successfully installed components from "Uncertain" to "Ready".

## What to do next

Restart the installation by running the same command and encryption key you used previously for installing the fix pack. Then select **resume previous install**. If you change the `install.props` file, start the fix pack installation again by selecting **start new install**.

**Note:** If you select **start new install**, ensure that you have clean servers, prepared as instructed for installing the fix pack, and all components are on.

When resuming an installation, you might receive the errors in the prerequisite check indicating servers are stopped, as follows:

```
CHK014E : Can not connect to WAS profile ISKMgr01 with on server XXX.  
CHK022E : WAS server MEMBER01 on profile ISKCustom01 is not started on server XXX.  
CHK022E : WAS server MEMBER02 on profile ISKCustom02 is not started on server XXX.
```

To restart the servers, log on to the analytic server as root and run these commands in sequence:

```
/opt/IBM/WebSphere/AppServer/profiles/ISKMgr01/bin/startManager.sh  
/opt/IBM/WebSphere/AppServer/profiles/ISKCustom01/bin/startNode.sh  
/opt/IBM/WebSphere/AppServer/profiles/ISKCustom01/bin/startServer.sh MEMBER01  
/opt/IBM/WebSphere/AppServer/profiles/ISKCustom02/bin/startNode.sh  
/opt/IBM/WebSphere/AppServer/profiles/ISKCustom02/bin/startServer.sh MEMBER02
```

### Related concepts:

“CHK: Installation prerequisite checking messages” on page 132

Use the information in this section to understand and respond to error, warning, and informational messages generated during the installation prerequisite checking process.

“Troubleshooting tips” on page 141

This section contains a list of commonly occurring problems and some troubleshooting tips for each item.

### Related tasks:

“Installing the fix pack” on page 41

Use the command line to install the IBM Intelligent Operations Center 1.0 Fix Pack 1.





---

## Chapter 9. References

These topics contain additional reference information to help you.

---

### PDF library

This topic provides links to the information center content in PDF format.

The information center content is available in the following PDF for convenient printing:

- IBM Intelligent Operations Center Information Center

---

### Additional information

The following additional resources are available online.

#### WebSphere Portal

- WebSphere Portal product support page: [http://www.ibm.com/support/entry/portal/Overview/Software/WebSphere/WebSphere\\_Portal](http://www.ibm.com/support/entry/portal/Overview/Software/WebSphere/WebSphere_Portal)
- WebSphere Portal information library: <http://www.ibm.com/software/genservers/portal/library/>
- WebSphere Portal wiki: <http://www.lotus.com/ldd/portalwiki.nsf>

#### WebSphere Application Server

- WebSphere Application Server product support page: <http://www.ibm.com/software/webservers/appserv/was/support/>
- WebSphere Application Server information library: <http://www.ibm.com/software/webservers/appserv/was/library/index.html>
- WebSphere Application Server 7.0.x Information Center: <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp>

#### Information centers

- WebSphere Application Server 7.0.x information center: <http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp>
- Tivoli Service Request Manager information center: [http://publib.boulder.ibm.com/infocenter/tivihelp/v32r1/index.jsp?topic=/com.ibm.srm.doc/srm\\_welcome.htm](http://publib.boulder.ibm.com/infocenter/tivihelp/v32r1/index.jsp?topic=/com.ibm.srm.doc/srm_welcome.htm)
- Lotus Notes information center: <http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp>
- WebSphere Message Broker information center: <http://publib.boulder.ibm.com/infocenter/wmbhelp/v7r0m0/index.jsp>
- IBM WebSphere Business Monitor information center: <http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r0mx/index.jsp?topic=/com.ibm.btools.help.monitor.doc/home/home.html>
- Rational Application Developer information center: [http://publib.boulder.ibm.com/infocenter/radhelp/v7r5/index.jsp?topic=/com.ibm.rad.legal.doc/helpindex\\_rad.html](http://publib.boulder.ibm.com/infocenter/radhelp/v7r5/index.jsp?topic=/com.ibm.rad.legal.doc/helpindex_rad.html)

#### Redbooks®

- Redbooks Domain: <http://publib-b.boulder.ibm.com/Redbooks.nsf>

#### Other web resources

- Tivoli training and certification: <http://www.ibm.com/software/tivoli/education/>
- OASIS Common Alerting Protocol Version 1.2 <http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html>

- Red Hat website: <http://www.redhat.com/>

---

## Copyright notice and trademarks

---

### Copyright notice

© Copyright IBM Corporation 2011, 2012. All rights reserved. May only be used pursuant to an IBM software license agreement. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without prior written permission of IBM Corporation. IBM Corporation grants you limited permission to make hardcopy or other reproductions of any machine-readable documentation for your own use, provided that each such reproduction shall carry the IBM Corporation copyright notice. No other rights under copyright are granted without prior written permission of IBM Corporation. The document is not intended for production and is furnished “as is” without warranty of any kind. **All warranties on this document are hereby disclaimed, including the warranty of non-infringement and the implied warranties of merchantability and fitness for a particular purpose.**

U.S. Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corporation.

---

### Trademarks

IBM, WebSphere, DB2, Rational, Tivoli, ibm.com, Passport Advantage, Sametime, and Redbooks are trademarks of the IBM Corporation in the United States, other countries, or both.

Microsoft, Internet Explorer, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Pentium is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Adobe, Acrobat, Portable Document Format (PDF), and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Oracle, Javascript, and Java are registered trademarks of Oracle and/or its affiliates.

ArcGIS, EDN, StreetMap, @esri.com, and www.esri.com are trademarks, registered trademarks, or service marks of Esri in the United States, the European Community, or certain other jurisdictions.

Other names may be trademarks of their respective owners. Other company, product, and service names may be trademarks or service marks of others.

---

## Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
1623-14, Shimotsuruma, Yamato-shi  
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation  
Department T81B F6/Building 503  
4205 S. Miami Boulevard  
Durham NC 27709-9990  
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, 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.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

---

## Trademarks

IBM, WebSphere, DB2, Rational, Tivoli, ibm.com, Passport Advantage, Sametime, and Redbooks are trademarks of the IBM Corporation in the United States, other countries, or both.

Microsoft, Internet Explorer, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Pentium is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Adobe, Acrobat, Portable Document Format (PDF), and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Oracle, Javascript, and Java are registered trademarks of Oracle and/or its affiliates.

ArcGIS, EDN, StreetMap, @esri.com, and www.esri.com are trademarks, registered trademarks, or service marks of Esri in the United States, the European Community, or certain other jurisdictions.

Other names may be trademarks of their respective owners. Other company, product, and service names may be trademarks or service marks of others.



---

## Index

### N

notices 146

### T

trademarks 146





---

## Readers' Comments — We'd Like to Hear from You

IBM Intelligent Operations Center  
IBM Intelligent Operations Center  
Product Documentation  
Version 1 Release 0

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:

- Send your comments to the address on the reverse side of this form.
- Send a fax to the following number: 1-800-227-5088 (US and Canada)

If you would like a response from IBM, please fill in the following information:

\_\_\_\_\_

Name

\_\_\_\_\_

Address

\_\_\_\_\_

Company or Organization

\_\_\_\_\_

Phone No.

\_\_\_\_\_

Email address



Fold and Tape

Please do not staple

Fold and Tape



NO POSTAGE  
NECESSARY  
IF MAILED IN THE  
UNITED STATES

# BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM  
Information Development Department DLUA  
P.O. Box 12195  
Research Triangle Park, NC  
USA 27709-9990



Fold and Tape

Please do not staple

Fold and Tape





Printed in USA